BigchainDB Server Documentation

Release 1.3.0

BigchainDB Contributors

Nov 21, 2017

Contents

1 Introduction 1

2 Quickstart 3

3 Production Nodes 5

4 Clusters 13

5 Production Deployment Template 15

6 Develop & Test BigchainDB Server 65

7 Settings & CLI 77

8 The HTTP Client-Server API 89

9 The Events API 109

10 Drivers & Tools 113

11 Data Models 115

12 Release Notes 125

13 Glossary 127

14 Appendices 129

Python Module Index 175

HTTP Routing Table 177

CHAPTER 1

Introduction

This is the documentation for BigchainDB Server, the BigchainDB software that one runs on servers (but not on clients).

If you want to use BigchainDB Server, then you should first understand what BigchainDB is, plus some of the specialized BigchaindB terminology. You can read about that in the overall BigchainDB project documentation.

Note that there are a few kinds of nodes:

- A **dev/test node** is a node created by a developer working on BigchainDB Server, e.g. for testing new or changed code. A dev/test node is typically run on the developer's local machine.
- A **bare-bones node** is a node deployed in the cloud, either as part of a testing cluster or as a starting point before upgrading the node to be production-ready.
- A **production node** is a node that is part of a consortium's BigchainDB cluster. A production node has the most components and requirements.

1.1 Setup Instructions for Various Cases

- Quickstart
- Set up a local BigchainDB node for development, experimenting and testing
- Set up and run a BigchainDB cluster

There are some old RethinkDB-based deployment instructions as well:

- Deploy a bare-bones RethinkDB-based node on Azure
- Deploy a RethinkDB-based testing cluster on AWS

Instructions for setting up a client will be provided once there's a public test net.

1.2 Can I Help?

Yes! BigchainDB is an open-source project; we welcome contributions of all kinds. If you want to request a feature, file a bug report, make a pull request, or help in some other way, please see the CONTRIBUTING.md file.

CHAPTER 2

Quickstart

This page has instructions to set up a single stand-alone BigchainDB node for learning or experimenting. Instructions for other cases are elsewhere. We will assume you're using Ubuntu 16.04 or similar. You can also try, running BigchainDB with Docker.

A. Install MongoDB as the database backend. (There are other options but you can ignore them for now.)

Install MongoDB Server 3.4+

B. To run MongoDB with default database path i.e. /data/db, open a Terminal and run the following command:

```
$ sudo mkdir -p /data/db
```

C. Assign rwx(read/write/execute) permissions to the user for default database directory:

```
$ sudo chmod -R 700 /data/db
```

D. Run MongoDB (but do not close this terminal):

```
$ sudo mongod --replSet=bigchain-rs
```

E. Ubuntu 16.04 already has Python 3.5, so you don't need to install it, but you do need to install some other things within a new terminal:

```
$ sudo apt-get update
$ sudo apt-get install libffi-dev libssl-dev
```

F. Get the latest version of pip and setuptools:

```
$ sudo apt-get install python3-pip
$ sudo pip3 install --upgrade pip setuptools
```

G. Install the `bigchaindb` Python package from PyPI:

```
$ sudo pip3 install bigchaindb
```

In case you are having problems with installation or package/module versioning, please upgrade the relevant packages on your host by running one the following commands:

```
$ sudo pip3 install [packageName]==[packageVersion]

OR

$ sudo pip3 install [packageName] --upgrade
```

H. Configure BigchainDB Server:

```
$ bigchaindb -y configure mongodb
```

I. Run BigchainDB Server:

```
$ bigchaindb start
```

J. Verify BigchainDB Server setup by visiting the BigchainDB Root URL in your browser:

http://127.0.0.1:9984/

A correctly installed installation will show you a JSON object with information about the API, docs, version and your public key.

You now have a running BigchainDB Server and can post transactions to it. One way to do that is to use the BigchainDB Python Driver.

Install the BigchainDB Python Driver (link)

CHAPTER 3

Production Nodes

3.1 Production Node Assumptions

Be sure you know the key BigchainDB terminology:

- BigchainDB node, BigchainDB cluster and BigchainDB consortum
- dev/test node, bare-bones node and production node

We make some assumptions about production nodes:

1. Production nodes use MongoDB, not RethinkDB.
2. Each production node is set up and managed by an experienced professional system administrator or a team of them.
3. Each production node in a cluster is managed by a different person or team.

You can use RethinkDB when building prototypes, but we don't advise or support using it in production.

We don't provide a detailed cookbook explaining how to secure a server, or other things that a sysadmin should know. We do provide some templates, but those are just starting points.

3.2 Production Node Components

A production BigchainDB node must include:

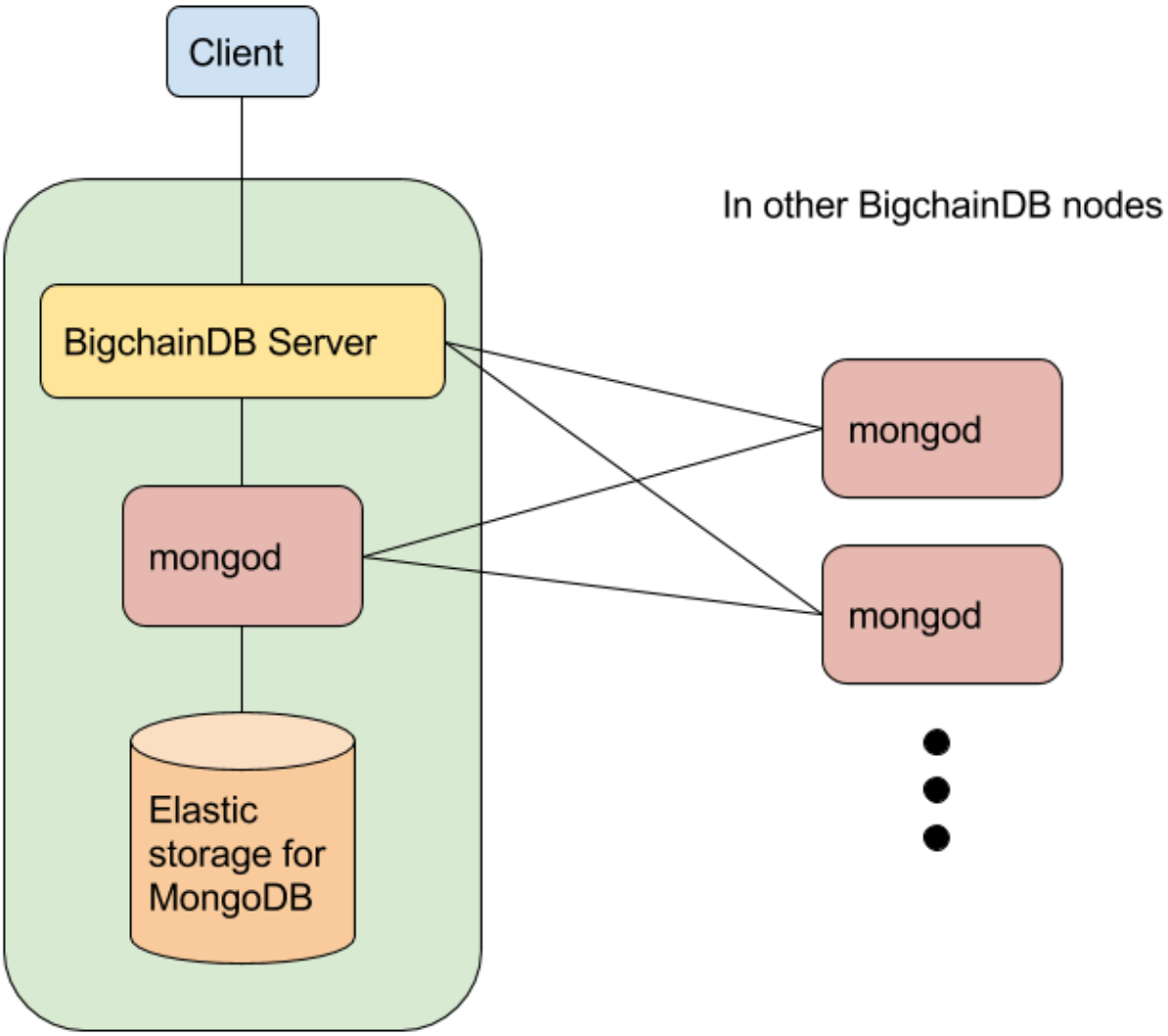
- BigchainDB Server
- MongoDB Server 3.4+ (mongod)
- Scalable storage for MongoDB

It could also include several other components, including:

- NGINX or similar, to provide authentication, rate limiting, etc.
- An NTP daemon running on all machines running BigchainDB Server or mongod, and possibly other machines

- **Not** MongoDB Automation Agent. It's for automating the deployment of an entire MongoDB cluster, not just one MongoDB node within a cluster.
- MongoDB Monitoring Agent
- MongoDB Backup Agent
- Log aggregation software
- Monitoring software
- Maybe more

The relationship between the main components is illustrated below. Note that BigchainDB Server must be able to communicate with the *primary* MongoDB instance, and any of the MongoDB instances might be the primary, so BigchainDB Server must be able to communicate with all the MongoDB instances. Also, all MongoDB instances must be able to communicate with each other.



3.3 Production Node Requirements

This page is about the requirements of BigchainDB Server. You can find the requirements of MongoDB, NGINX, your NTP daemon, your monitoring software, and other production node components in the documentation for that software.

3.3.1 OS Requirements

BigchainDB Server requires Python 3.5+ and Python 3.5+ will run on any modern OS, but we recommend using an LTS version of Ubuntu Server or a similarly server-grade Linux distribution.

Don't use macOS (formerly OS X, formerly Mac OS X), because it's not a server-grade operating system. Also, BigchaindB Server uses the Python multiprocessing package and some functionality in the multiprocessing package doesn't work on Mac OS X.

3.3.2 General Considerations

BigchainDB Server runs many concurrent processes, so more RAM and more CPU cores is better.

As mentioned on the page about production node components, every machine running BigchainDB Server should be running an NTP daemon.

3.4 Set Up and Run a Cluster Node

This is a page of general guidelines for setting up a production BigchainDB node. Before continuing, make sure you've read the pages about production node assumptions, components and requirements.

Note: These are just guidelines. You can modify them to suit your needs. For example, if you want to initialize the MongoDB replica set before installing BigchainDB, you *can* do that. If you'd prefer to use Docker and Kubernetes, you can (and we have a template). We don't cover all possible setup procedures here.

3.4.1 Security Guidelines

There are many articles, websites and books about securing servers, virtual machines, networks, etc. Consult those. There are some notes on BigchainDB-specific firewall setup in the Appendices.

3.4.2 Sync Your System Clock

A BigchainDB node uses its system clock to generate timestamps for blocks and votes, so that clock should be kept in sync with some standard clock(s). The standard way to do that is to run an NTP daemon (Network Time Protocol daemon) on the node.

MongoDB also recommends having an NTP daemon running on all MongoDB nodes.

NTP is a standard protocol. There are many NTP daemons implementing it. We don't recommend a particular one. On the contrary, we recommend that different nodes in a cluster run different NTP daemons, so that a problem with one daemon won't affect all nodes.

Please see the notes on NTP daemon setup in the Appendices.

3.4.3 Set Up Storage for MongoDB

We suggest you set up a separate storage device (partition, RAID array, or logical volume) to store the data in the MongoDB database. Here are some questions to ask:

- How easy will it be to add storage in the future? Will I have to shut down my server?
- How big can the storage get? (Remember that RAID can be used to make several physical drives look like one.)
- How fast can it read & write data? How many input/output operations per second (IOPS)?
- How does IOPS scale as more physical hard drives are added?
- What's the latency?
- What's the reliability? Is there replication?
- What's in the Service Level Agreement (SLA), if applicable?
- What's the cost?

There are many options and tradeoffs.

Consult the MongoDB documentation for its recommendations regarding storage hardware, software and settings, e.g. in the MongoDB Production Notes.

3.4.4 Install and Run MongoDB

- Install MongoDB 3.4+. (BigchainDB only works with MongoDB 3.4+.)
- Run MongoDB (mongod)

3.4.5 Install BigchainDB Server

Install BigchainDB Server Dependencies

Before you can install BigchainDB Server, you must install its OS-level dependencies and you may have to install Python 3.5+.

How to Install BigchainDB Server with pip

BigchainDB is distributed as a Python package on PyPI so you can install it using `pip`. First, make sure you have an up-to-date Python 3.5+ version of `pip` installed:

```
pip -V
```

If it says that `pip` isn't installed, or it says `pip` is associated with a Python version less than 3.5, then you must install a `pip` version associated with Python 3.5+. In the following instructions, we call it `pip3` but you may be able to use `pip` if that refers to the same thing. See the `pip` installation instructions.

On Ubuntu 16.04, we found that this works:

```
sudo apt-get install python3-pip
```

That should install a Python 3 version of `pip` named `pip3`. If that didn't work, then another way to get `pip3` is to do `sudo apt-get install python3-setuptools` followed by `sudo easy_install3 pip`.

You can upgrade `pip` (`pip3`) and `setuptools` to the latest versions using:

```
pip3 install --upgrade pip setuptools
pip3 -V
```

Now you can install BigchainDB Server using:

```
pip3 install bigchaindb
```

(If you're not in a virtualenv and you want to install bigchaindb system-wide, then put `sudo` in front.)

Note: You can use `pip3` to upgrade the `bigchaindb` package to the latest version using `pip3 install --upgrade bigchaindb`.

How to Install BigchainDB Server from Source

If you want to install BitchainDB from source because you want to use the very latest bleeding-edge code, clone the public repository:

```
git clone git@github.com:bigchaindb/bigchaindb.git
cd bigchaindb
python setup.py install
```

3.4.6 Configure BigchainDB Server

Start by creating a default BigchainDB config file for a MongoDB backend:

```
bigchaindb -y configure mongodb
```

(There's documentation for the `bigchaindb` command is in the section on the BigchainDB Command Line Interface (CLI).)

Edit the created config file by opening `$HOME/.bigchaindb` (the created config file) in your text editor:

- Change `"server": {"bind": "localhost:9984", ... }` to `"server": {"bind": "0.0.0.0:9984", ... }`. This makes it so traffic can come from any IP address to port 9984 (the HTTP Client-Server API port).
- Change `"keyring": []` to `"keyring": ["public_key_of_other_node_A", "public_key_of_other_node_B", "..."]` i.e. a list of the public keys of all the other nodes in the cluster. The keyring should *not* include your node's public key.
- Ensure that `database.host` and `database.port` are set to the hostname and port of your MongoDB instance. (The port is usually 27017, unless you changed it.)

For more information about the BigchainDB config file, see the page about the BigchainDB configuration settings.

3.4.7 Get All Other Nodes to Update Their Keyring

All other BigchainDB nodes in the cluster must add your new node's public key to their BigchainDB keyring. Currently, the only way to get BigchainDB Server to "notice" a changed keyring is to shut it down and start it back up again (with the new keyring).

3.4.8 Maybe Update the MongoDB Replica Set

If this isn't the first node in the BigchainDB cluster, then someone with an existing BigchainDB node (not you) must add your MongoDB instance to the MongoDB replica set. They can do so (on their node) using:

```
bigchaindb add-replicas your-mongod-hostname:27017
```

where they must replace `your-mongod-hostname` with the actual hostname of your MongoDB instance, and they may have to replace `27017` with the actual port.

3.4.9 Start BigchainDB

Warning: If you're not deploying the first node in the BigchainDB cluster, then don't start BigchainDB before your MongoDB instance has been added to the MongoDB replica set (as outlined above).

```
# See warning above
bigchaindb start
```

3.5 Using a Reverse Proxy

You may want to:

- rate limit inbound HTTP requests,
- authenticate/authorize inbound HTTP requests,
- block requests with an HTTP request body that's too large, or
- enable HTTPS (TLS) between your users and your node.

While we could have built all that into BigchainDB Server, we didn't, because you can do all that (and more) using a reverse proxy such as NGINX or HAProxy. (You would put it in front of your BigchainDB Server, so that all inbound HTTP requests would arrive at the reverse proxy before *maybe* being proxied onwards to your BigchainDB Server.) For detailed instructions, see the documentation for your reverse proxy.

Below, we note how a reverse proxy can be used to do some BigchainDB-specific things.

You may also be interested in our NGINX configuration file template (open source, on GitHub).

3.5.1 Enforcing a Max Transaction Size

The BigchainDB HTTP API has several endpoints, but only one of them, the `POST /transactions` endpoint, expects a non-empty HTTP request body: the transaction (JSON) being submitted by the user.

If you want to enforce a maximum-allowed transaction size (discarding any that are larger), then you can do so by configuring a maximum request body size in your reverse proxy. For example, NGINX has the `client_max_body_size` configuration setting. You could set it to 15 kB with the following line in your NGINX config file:

```
client_max_body_size 15k;
```

For more information, see the NGINX docs about client_max_body_size.

Note: By enforcing a maximum transaction size, you indirectly enforce a maximum crypto-conditions complexity.

Aside: Why 15 kB?

Both RethinkDB and MongoDB have a maximum document size of 16 MB. In BigchainDB, the biggest documents are the blocks. A BigchainDB block can contain up to 1000 transactions, plus some other data (e.g. the timestamp). If we ignore the other data as negligible relative to all the transactions, then a block of size 16 MB will have an average transaction size of (16 MB)/1000 = 16 kB. Therefore by limiting the max transaction size to 15 kB, you can be fairly sure that no blocks will ever be bigger than 16 MB.

Note: Technically, the documents that MongoDB stores aren't the JSON that BigchainDB users think of; they're JSON converted to BSON. Moreover, one can use GridFS with MongoDB to store larger documents. Therefore the above calculation shoud be seen as a rough guide, not the last word.

CHAPTER 4

Clusters

A **BigchainDB Cluster** is a set of connected **BigchainDB Nodes**, managed by a **BigchainDB Consortium** (i.e. an organization). Those terms are defined in the BigchainDB Terminology page.

4.1 Consortium Structure & Governance

The consortium might be a company, a foundation, a cooperative, or some other form of organization. It must make many decisions, e.g. How will new members be added? Who can read the stored data? What kind of data will be stored? A governance process is required to make those decisions, and therefore one of the first steps for any new consortium is to specify its governance process (if one doesn't already exist). This documentation doesn't explain how to create a consortium, nor does it outline the possible governance processes.

It's worth noting that the decentralization of a BigchainDB cluster depends, to some extent, on the decentralization of the associated consortium. See the pages about decentralization and node diversity.

4.2 Relevant Technical Documentation

There are some pages and sections that will be of particular interest to anyone building or managing a BigchainDB cluster. In particular:

- the page about how to set up and run a cluster node,
- our production deployment template, and
- our old RethinkDB-based AWS deployment template.

4.3 Cluster DNS Records and SSL Certificates

We now describe how *we* set up the external (public-facing) DNS records for a BigchainDB cluster. Your consortium may opt to do it differently. There were several goals:

- Allow external users/clients to connect directly to any BigchainDB node in the cluster (over the internet), if they want.
- Each BigchainDB node operator should get an SSL certificate for their BigchainDB node, so that their BigchainDB node can serve the BigchainDB HTTP API via HTTPS. (The same certificate might also be used to serve the WebSocket API.)
- There should be no sharing of SSL certificates among BigchainDB node operators.
- Optional: Allow clients to connect to a "random" BigchainDB node in the cluster at one particular domain (or subdomain).

4.3.1 Node Operator Responsibilities

1. Register a domain (or use one that you already have) for your BigchainDB node. You can use a subdomain if you like. For example, you might opt to use `abc-org73.net`, `api.dynabob8.io` or `figmentdb3.ninja`.
2. Get an SSL certificate for your domain or subdomain, and properly install it in your node (e.g. in your NGINX instance).
3. Create a DNS A Record mapping your domain or subdomain to the public IP address of your node (i.e. the one that serves the BigchainDB HTTP API).

4.3.2 Consortium Responsibilities

Optional: The consortium managing the BigchainDB cluster could register a domain name and set up CNAME records mapping that domain name (or one of its subdomains) to each of the nodes in the cluster. For example, if the consortium registered `bdbcluster.io`, they could set up CNAME records like the following:

- CNAME record mapping `api.bdbcluster.io` to `abc-org73.net`
- CNAME record mapping `api.bdbcluster.io` to `api.dynabob8.io`
- CNAME record mapping `api.bdbcluster.io` to `figmentdb3.ninja`

CHAPTER 5

Production Deployment Template

This section outlines how *we* deploy production BigchainDB nodes and clusters on Microsoft Azure using Kubernetes. We improve it constantly. You may choose to use it as a template or reference for your own deployment, but *we make no claim that it is suitable for your purposes*. Feel free change things to suit your needs or preferences.

5.1 Overview

This page summarizes the steps *we* go through to set up a production BigchainDB cluster. We are constantly improving them. You can modify them to suit your needs.

5.1.1 Things the Managing Organization Must Do First

1. Set Up a Self-Signed Certificate Authority

We use SSL/TLS and self-signed certificates for MongoDB authentication (and message encryption). The certificates are signed by the organization managing the cluster. If your organization already has a process for signing certificates (i.e. an internal self-signed certificate authority [CA]), then you can skip this step. Otherwise, your organization must *set up its own self-signed certificate authority*.

2. Register a Domain and Get an SSL Certificate for It

The BigchainDB APIs (HTTP API and WebSocket API) should be served using TLS, so the organization running the cluster should choose an FQDN for their API (e.g. api.organization-x.com), register the domain name, and buy an SSL/TLS certificate for the FQDN.

5.1.2 Things Each Node Operator Must Do

Every MongoDB instance in the cluster must have a unique (one-of-a-kind) name. Ask the organization managing your cluster if they have a standard way of naming instances in the cluster. For example, maybe they assign a unique number

to each node, so that if you're operating node 12, your MongoDB instance would be named `mdb-instance-12`. Similarly, other instances must also have unique names in the cluster.

1. Name of the MongoDB instance (`mdb-instance-*`)
2. Name of the BigchainDB instance (`bdb-instance-*`)
3. Name of the NGINX instance (`ngx-http-instance-*` or `ngx-https-instance-*`)
4. Name of the OpenResty instance (`openresty-instance-*`)
5. Name of the MongoDB monitoring agent instance (`mdb-mon-instance-*`)
6. Name of the MongoDB backup agent instance (`mdb-bak-instance-*`)

Generate four keys and corresponding certificate signing requests (CSRs):

1. Server Certificate (a.k.a. Member Certificate) for the MongoDB instance
2. Client Certificate for BigchainDB Server to identify itself to MongoDB
3. Client Certificate for MongoDB Monitoring Agent to identify itself to MongoDB
4. Client Certificate for MongoDB Backup Agent to identify itself to MongoDB

Ask the managing organization to use its self-signed CA to sign those four CSRs. They should send you:

- Four certificates (one for each CSR you sent them).
- One `ca.crt` file: their CA certificate.
- One `crl.pem` file: a certificate revocation list.

For help, see the pages:

- *How to Generate a Server Certificate for MongoDB*
- *How to Generate a Client Certificate for MongoDB*

Every node in a BigchainDB cluster needs its own BigchainDB keypair (i.e. a public key and corresponding private key). You can generate a BigchainDB keypair for your node, for example, using the BigchainDB Python Driver.

```
from bigchaindb_driver.crypto import generate_keypair
print(generate_keypair())
```

Share your BigchaindB *public* key with all the other nodes in the BigchainDB cluster. Don't share your private key.

Get the BigchainDB public keys of all the other nodes in the cluster. That list of public keys is known as the BigchainDB "keyring."

Make up an FQDN for your BigchainDB node (e.g. `mynode.mycorp.com`). Make sure you've registered the associated domain name (e.g. `mycorp.com`), and have an SSL certificate for the FQDN. (You can get an SSL certificate from any SSL certificate provider.)

Ask the managing organization for the user name to use for authenticating to MongoDB.

If the cluster uses 3scale for API authentication, monitoring and billing, you must ask the managing organization for all relevant 3scale credentials - secret token, service ID, version header and API service token.

If the cluster uses MongoDB Cloud Manager for monitoring and backup, you must ask the managing organization for the `Project ID` and the `Agent API Key`. (Each Cloud Manager "Project" has its own `Project ID`. A `Project ID` can contain a number of `Agent API Key` s. It can be found under **Settings**. It was recently added to the Cloud Manager to allow easier periodic rotation of the `Agent API Key` with a constant `Project ID`)

Deploy a Kubernetes cluster on Azure.

You can now proceed to set up your BigchainDB node based on whether it is the *first node in a new cluster* or a *node that will be added to an existing cluster*.

5.2 How to Set Up a Self-Signed Certificate Authority

This page enumerates the steps *we* use to set up a self-signed certificate authority (CA). This is something that only needs to be done once per cluster, by the organization managing the cluster, i.e. the CA is for the whole cluster. We use Easy-RSA.

5.2.1 Step 1: Install & Configure Easy-RSA

First create a directory for the CA and cd into it:

```
mkdir bdb-cluster-ca

cd bdb-cluster-ca
```

Then *install and configure Easy-RSA in that directory*.

5.2.2 Step 2: Create a Self-Signed CA

You can create a self-signed CA by going to the `bdb-cluster-ca/easy-rsa-3.0.1/easyrsa3` directory and using:

```
./easyrsa init-pki

./easyrsa build-ca
```

You will also be asked to enter a PEM pass phrase (for encrypting the `ca.key` file). Make sure to securely store that PEM pass phrase. If you lose it, you won't be able to add or remove entities from your PKI infrastructure in the future.

You will be prompted to enter the Distinguished Name (DN) information for this CA. For each field, you can accept the default value [in brackets] by pressing Enter.

> **Warning:** Don't accept the default value of OU (`IT`). Instead, enter the value `ROOT-CA`.

While `Easy-RSA CA` *is* a valid and acceptable Common Name, you should probably enter a name based on the name of the managing organization, e.g. `Omega Ledger CA`.

Tip: You can get help with the `easyrsa` command (and its subcommands) by using the subcommand `./easyrsa help`

5.2.3 Step 3: Create an Intermediate CA

TODO

5.2.4 Step 4: Generate a Certificate Revocation List

You can generate a Certificate Revocation List (CRL) using:

```
./easyrsa gen-crl
```

You will need to run this command every time you revoke a certificate. The generated `crl.pem` needs to be uploaded to your infrastructure to prevent the revoked certificate from being used again.

5.2.5 Step 5: Secure the CA

The security of your infrastructure depends on the security of this CA.

- Ensure that you restrict access to the CA and enable only legitimate and required people to sign certificates and generate CRLs.
- Restrict access to the machine where the CA is hosted.
- Many certificate providers keep the CA offline and use a rotating intermediate CA to sign and revoke certificates, to mitigate the risk of the CA getting compromised.
- In case you want to destroy the machine where you created the CA (for example, if this was set up on a cloud provider instance), you can backup the entire `easyrsa` directory to secure storage. You can always restore it to a trusted instance again during the times when you want to sign or revoke certificates. Remember to backup the directory after every update.

5.3 How to Generate a Server Certificate for MongoDB

This page enumerates the steps *we* use to generate a server certificate for a MongoDB instance. A server certificate is also referred to as a "member certificate" in the MongoDB documentation. We use Easy-RSA.

5.3.1 Step 1: Install & Configure Easy–RSA

First create a directory for the server certificate (member cert) and cd into it:

```
mkdir member-cert

cd member-cert
```

Then *install and configure Easy-RSA in that directory*.

5.3.2 Step 2: Create the Server Private Key and CSR

You can create the server private key and certificate signing request (CSR) by going into the directory `member-cert/easy-rsa-3.0.1/easyrsa3` and using something like:

Note: Please make sure you are fullfilling the requirements for MongoDB server/member certificates.

```
./easyrsa init-pki

./easyrsa --req-cn=mdb-instance-0 --subject-alt-name=DNS:localhost,DNS:mdb-instance-0␣
↪gen-req mdb-instance-0 nopass
```

You should replace the Common Name (`mdb-instance-0` above) with the correct name for *your* MongoDB instance in the cluster, e.g. `mdb-instance-5` or `mdb-instance-12`. (This name is decided by the organization managing the cluster.)

You will be prompted to enter the Distinguished Name (DN) information for this certificate. For each field, you can accept the default value [in brackets] by pressing Enter.

Warning: Don't accept the default value of OU (`IT`). Instead, enter the value `MongoDB-Instance`.

Aside: You need to provide the `DNS:localhost` SAN during certificate generation for using the `localhost exception` in the MongoDB instance. All certificates can have this attribute without compromising security as the `localhost exception` works only the first time.

5.3.3 Step 3: Get the Server Certificate Signed

The CSR file created in the last step should be located in `pki/reqs/mdb-instance-0.req` (where the integer `0` may be different for you). You need to send it to the organization managing the cluster so that they can use their CA to sign the request. (The managing organization should already have a self-signed CA.)

If you are the admin of the managing organization's self-signed CA, then you can import the CSR and use Easy-RSA to sign it. Go to your `bdb-cluster-ca/easy-rsa-3.0.1/easyrsa3/` directory and do something like:

```
./easyrsa import-req /path/to/mdb-instance-0.req mdb-instance-0

./easyrsa --subject-alt-name=DNS:localhost,DNS:mdb-instance-0 sign-req server mdb-
↪instance-0
```

Once you have signed it, you can send the signed certificate and the CA certificate back to the requestor. The files are `pki/issued/mdb-instance-0.crt` and `pki/ca.crt`.

5.3.4 Step 4: Generate the Consolidated Server PEM File

MongoDB requires a single, consolidated file containing both the public and private keys.

```
cat /path/to/mdb-instance-0.crt /path/to/mdb-instance-0.key > mdb-instance-0.pem
```

5.4 How to Generate a Client Certificate for MongoDB

This page enumerates the steps *we* use to generate a client certificate to be used by clients who want to connect to a TLS-secured MongoDB cluster. We use Easy-RSA.

5.4.1 Step 1: Install and Configure Easy-RSA

First create a directory for the client certificate and cd into it:

```
mkdir client-cert

cd client-cert
```

Then *install and configure Easy-RSA in that directory*.

5.4.2 Step 2: Create the Client Private Key and CSR

You can create the client private key and certificate signing request (CSR) by going into the directory `client-cert/easy-rsa-3.0.1/easyrsa3` and using:

```
./easyrsa init-pki

./easyrsa gen-req bdb-instance-0 nopass
```

You should change the Common Name (e.g. `bdb-instance-0`) to a value that reflects what the client certificate is being used for, e.g. `mdb-mon-instance-3` or `mdb-bak-instance-4`. (The final integer is specific to your BigchainDB node in the BigchainDB cluster.)

You will be prompted to enter the Distinguished Name (DN) information for this certificate. For each field, you can accept the default value [in brackets] by pressing Enter.

Warning: Don't accept the default value of OU (`IT`). Instead, enter the value `BigchainDB-Instance`, `MongoDB-Mon-Instance` or `MongoDB-Backup-Instance` as appropriate.

Aside: The `nopass` option means "do not encrypt the private key (default is encrypted)". You can get help with the `easyrsa` command (and its subcommands) by using the subcommand `./easyrsa help`.

Note: For more information about requirements for MongoDB client certificates, please consult the official MongoDB documentation.

5.4.3 Step 3: Get the Client Certificate Signed

The CSR file created in the previous step should be located in `pki/reqs/bdb-instance-0.req` (or whatever Common Name you used in the `gen-req` command above). You need to send it to the organization managing the cluster so that they can use their CA to sign the request. (The managing organization should already have a self-signed CA.)

If you are the admin of the managing organization's self-signed CA, then you can import the CSR and use Easy-RSA to sign it. Go to your `bdb-cluster-ca/easy-rsa-3.0.1/easyrsa3/` directory and do something like:

```
./easyrsa import-req /path/to/bdb-instance-0.req bdb-instance-0

./easyrsa sign-req client bdb-instance-0
```

Once you have signed it, you can send the signed certificate and the CA certificate back to the requestor. The files are `pki/issued/bdb-instance-0.crt` and `pki/ca.crt`.

5.4.4 Step 4: Generate the Consolidated Client PEM File

Note: This step can be skipped for BigchainDB client certificate as BigchainDB uses the PyMongo driver, which accepts separate certificate and key files.

MongoDB, MongoDB Backup Agent and MongoDB Monitoring Agent require a single, consolidated file containing both the public and private keys.

```
cat /path/to/bdb-instance-0.crt /path/to/bdb-instance-0.key > bdb-instance-0.pem

 OR

cat /path/to/mdb-mon-instance-0.crt /path/to/mdb-mon-instance-0.key > mdb-mon-
↪instance-0.pem

 OR

cat /path/to/mdb-bak-instance-0.crt /path/to/mdb-bak-instance-0.key > mdb-bak-
↪instance-0.pem
```

5.5 How to Revoke an SSL/TLS Certificate

This page enumerates the steps *we* take to revoke a self-signed SSL/TLS certificate in a cluster. It can only be done by someone with access to the self-signed CA associated with the cluster's managing organization.

5.5.1 Step 1: Revoke a Certificate

Since we used Easy-RSA version 3 to *set up the CA*, we use it to revoke certificates too.

Go to the following directory (associated with the self-signed CA): `.../bdb-cluster-ca/easy-rsa-3.0.1/easyrsa3`. You need to be aware of the file name used to import the certificate using the `./easyrsa import-req` before. Run the following command to revoke a certificate:

```
./easyrsa revoke <filename>
```

This will update the CA database with the revocation details. The next step is to use the updated database to issue an up-to-date certificate revocation list (CRL).

5.5.2 Step 2: Generate a New CRL

Generate a new CRL for your infrastructure using:

```
./easyrsa gen-crl
```

The generated `crl.pem` file needs to be uploaded to your infrastructure to prevent the revoked certificate from being used again.

In particlar, the generated `crl.pem` file should be sent to all BigchainDB node operators in your BigchainDB cluster, so that they can update it in their MongoDB instance and their BigchainDB Server instance.

5.6 Template: Deploy a Kubernetes Cluster on Azure

A BigchainDB node can be run inside a Kubernetes cluster. This page describes one way to deploy a Kubernetes cluster on Azure.

5.6.1 Step 1: Get a Pay-As-You-Go Azure Subscription

Microsoft Azure has a Free Trial subscription (at the time of writing), but it's too limited to run an advanced BigchainDB node. Sign up for a Pay-As-You-Go Azure subscription via the Azure website.

You may find that you have to sign up for a Free Trial subscription first. That's okay: you can have many subscriptions.

5.6.2 Step 2: Create an SSH Key Pair

You'll want an SSH key pair so you'll be able to SSH to the virtual machines that you'll deploy in the next step. (If you already have an SSH key pair, you *could* reuse it, but it's probably a good idea to make a new SSH key pair for your Kubernetes VMs and nothing else.)

See the *page about how to generate a key pair for SSH*.

5.6.3 Step 3: Deploy an Azure Container Service (ACS)

It's *possible* to deploy an Azure Container Service (ACS) from the Azure Portal (i.e. online in your web browser) but it's actually easier to do it using the Azure Command-Line Interface (CLI).

Microsoft has instructions to install the Azure CLI 2.0 on most common operating systems. Do that.

If you already *have* the Azure CLI installed, you may want to update it.

> **Warning:** `az component update` isn't supported if you installed the CLI using some of Microsoft's provided installation instructions. See the Microsoft docs for update instructions.

Next, login to your account using:

```
$ az login
```

It will tell you to open a web page and to copy a code to that page.

If the login is a success, you will see some information about all your subscriptions, including the one that is currently enabled (`"state": "Enabled"`). If the wrong one is enabled, you can switch to the right one using:

```
$ az account set --subscription <subscription name or ID>
```

Next, you will have to pick the Azure data center location where you'd like to deploy your cluster. You can get a list of all available locations using:

```
$ az account list-locations
```

Next, create an Azure "resource group" to contain all the resources (virtual machines, subnets, etc.) associated with your soon-to-be-deployed cluster. You can name it whatever you like but avoid fancy characters because they may confuse some software.

```
$ az group create --name <resource group name> --location <location name>
```

Example location names are `koreacentral` and `westeurope`.

Finally, you can deploy an ACS using something like:

```
$ az acs create --name <a made-up cluster name> \
--resource-group <name of resource group created earlier> \
--master-count 3 \
--agent-count 2 \
--admin-username ubuntu \
--agent-vm-size Standard_D2_v2 \
--dns-prefix <make up a name> \
--ssh-key-value ~/.ssh/<name>.pub \
--orchestrator-type kubernetes \
--debug --output json
```

Note: Please refer to Azure documentation for a comprehensive list of options available for *az acs create*. Please tune the following parameters as per your requirement:

- Master count.
- Agent count.
- Agent VM size.
- **Optional**: Master storage profile.
- **Optional**: Agent storage profile.

There are more options. For help understanding all the options, use the built-in help:

```
$ az acs create --help
```

It takes a few minutes for all the resources to deploy. You can watch the progress in the Azure Portal: go to **Resource groups** (with the blue cube icon) and click on the one you created to see all the resources in it.

5.6.4 Optional: SSH to Your New Kubernetes Cluster Nodes

You can SSH to one of the just-deployed Kubernetes "master" nodes (virtual machines) using:

```
$ ssh -i ~/.ssh/<name> ubuntu@<master-ip-address-or-fqdn>
```

where you can get the IP address or FQDN of a master node from the Azure Portal. For example:

```
$ ssh -i ~/.ssh/mykey123 ubuntu@mydnsprefix.westeurope.cloudapp.azure.com
```

Note: All the master nodes are accessible behind the *same* public IP address and FQDN. You connect to one of the masters randomly based on the load balancing policy.

The "agent" nodes shouldn't get public IP addresses or externally accessible FQDNs, so you can't SSH to them *directly*, but you can first SSH to the master and then SSH to an agent from there using their hostname. To do that, you could copy your SSH key pair to the master (a bad idea), or use SSH agent forwarding (better). To do the latter, do the following on the machine you used to SSH to the master:

```
$ echo -e "Host <FQDN of the cluster from Azure Portal>\n  ForwardAgent yes" >> ~/.
↪ssh/config
```

To verify that SSH agent forwarding works properly, SSH to the one of the master nodes and do:

```
$ echo "$SSH_AUTH_SOCK"
```

If you get an empty response, then SSH agent forwarding hasn't been set up correctly. If you get a non-empty response, then SSH agent forwarding should work fine and you can SSH to one of the agent nodes (from a master) using:

```
$ ssh ubuntu@k8s-agent-4AC80E97-0
```

where `k8s-agent-4AC80E97-0` is the name of a Kubernetes agent node in your Kubernetes cluster. You will have to replace it by the name of an agent node in your cluster.

5.6.5 Optional: Delete the Kubernetes Cluster

```
$ az acs delete \
--name <ACS cluster name> \
--resource-group <name of resource group containing the cluster>
```

5.6.6 Optional: Delete the Resource Group

CAUTION: You might end up deleting resources other than the ACS cluster.

```
$ az group delete \
--name <name of resource group containing the cluster>
```

Next, you can *run a BigchainDB node on your new Kubernetes cluster*.

5.7 Kubernetes Template: Deploy a Single BigchainDB Node

This page describes how to deploy the first BigchainDB node in a BigchainDB cluster, or a stand-alone BigchainDB node, using Kubernetes. It assumes you already have a running Kubernetes cluster.

If you want to add a new BigchainDB node to an existing BigchainDB cluster, refer to *the page about that*.

Below, we refer to many files by their directory and filename, such as `configuration/config-map.yaml`. Those files are files in the bigchaindb/bigchaindb repository on GitHub in the `k8s/` directory. Make sure you're getting those files from the appropriate Git branch on GitHub, i.e. the branch for the version of BigchainDB that your BigchainDB cluster is using.

5.7.1 Step 1: Install and Configure kubectl

kubectl is the Kubernetes CLI. If you don't already have it installed, then see the Kubernetes docs to install it.

The default location of the kubectl configuration file is `~/.kube/config`. If you don't have that file, then you need to get it.

Azure. If you deployed your Kubernetes cluster on Azure using the Azure CLI 2.0 (as per *our template*), then you can get the `~/.kube/config` file using:

```
$ az acs kubernetes get-credentials \
--resource-group <name of resource group containing the cluster> \
--name <ACS cluster name>
```

If it asks for a password (to unlock the SSH key) and you enter the correct password, but you get an error message, then try adding `--ssh-key-file ~/.ssh/<name>` to the above command (i.e. the path to the private key).

Note: About kubectl contexts. You might manage several Kubernetes clusters. To make it easy to switch from one to another, kubectl has a notion of "contexts," e.g. the context for cluster 1 or the context for cluster 2. To find out the current context, do:

```
$ kubectl config view
```

and then look for the `current-context` in the output. The output also lists all clusters, contexts and users. (You might have only one of each.) You can switch to a different context using:

```
$ kubectl config use-context <new-context-name>
```

You can also switch to a different context for just one command by inserting `--context <context-name>` into any kubectl command. For example:

```
$ kubectl --context k8s-bdb-test-cluster-0 get pods
```

will get a list of the pods in the Kubernetes cluster associated with the context named `k8s-bdb-test-cluster-0`.

5.7.2 Step 2: Connect to Your Cluster's Web UI (Optional)

You can connect to your cluster's Kubernetes Dashboard (also called the Web UI) using:

```
$ kubectl proxy -p 8001

or

$ az acs kubernetes browse -g [Resource Group] -n [Container service instance name] --
↪ssh-key-file /path/to/privateKey
```

or, if you prefer to be explicit about the context (explained above):

```
$ kubectl --context k8s-bdb-test-cluster-0 proxy -p 8001
```

The output should be something like `Starting to serve on 127.0.0.1:8001`. That means you can visit the dashboard in your web browser at http://127.0.0.1:8001/ui.

5.7.3 Step 3: Configure Your BigchainDB Node

See the page titled *How to Configure a BigchainDB Node*.

5.7.4 Step 4: Start the NGINX Service

- This will will give us a public IP for the cluster.
- Once you complete this step, you might need to wait up to 10 mins for the public IP to be assigned.
- You have the option to use vanilla NGINX without HTTPS support or an NGINX with HTTPS support.

Step 4.1: Vanilla NGINX

- This configuration is located in the file `nginx-http/nginx-http-svc.yaml`.
- Set the `metadata.name` and `metadata.labels.name` to the value set in `ngx-instance-name` in the ConfigMap above.
- Set the `spec.selector.app` to the value set in `ngx-instance-name` in the ConfigMap followed by `-dep`. For example, if the value set in the `ngx-instance-name` is `ngx-http-instance-0`, set the `spec.selector.app` to `ngx-http-instance-0-dep`.
- Set `ports[0].port` and `ports[0].targetPort` to the value set in the `cluster-frontend-port` in the ConfigMap above. This is the `public-cluster-port` in the file which is the ingress in to the cluster.
- Start the Kubernetes Service:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f nginx-http/nginx-http-svc.yaml
```

Step 4.2: NGINX with HTTPS

- You have to enable HTTPS for this one and will need an HTTPS certificate for your domain.
- You should have already created the necessary Kubernetes Secrets in the previous step (i.e. `https-certs`).
- This configuration is located in the file `nginx-https/nginx-https-svc.yaml`.
- Set the `metadata.name` and `metadata.labels.name` to the value set in `ngx-instance-name` in the ConfigMap above.
- Set the `spec.selector.app` to the value set in `ngx-instance-name` in the ConfigMap followed by `-dep`. For example, if the value set in the `ngx-instance-name` is `ngx-https-instance-0`, set the `spec.selector.app` to `ngx-https-instance-0-dep`.
- Set `ports[0].port` and `ports[0].targetPort` to the value set in the `cluster-frontend-port` in the ConfigMap above. This is the `public-secure-cluster-port` in the file which is the ingress in to the cluster.
- Set `ports[1].port` and `ports[1].targetPort` to the value set in the `mongodb-frontend-port` in the ConfigMap above. This is the `public-mdb-port` in the file which specifies where MongoDB is available.
- Start the Kubernetes Service:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f nginx-https/nginx-https-svc.
↪yaml
```

5.7.5 Step 5: Assign DNS Name to the NGINX Public IP

- This step is required only if you are planning to set up multiple BigchainDB nodes or are using HTTPS certificates tied to a domain.
- The following command can help you find out if the NGINX service started above has been assigned a public IP or external IP address:

```
$ kubectl --context k8s-bdb-test-cluster-0 get svc -w
```

- Once a public IP is assigned, you can map it to a DNS name. We usually assign `bdb-test-cluster-0`, `bdb-test-cluster-1` and so on in our documentation. Let's assume that we assign the unique name of `bdb-test-cluster-0` here.

Set up DNS mapping in Azure. Select the current Azure resource group and look for the `Public IP` resource. You should see at least 2 entries there - one for the Kubernetes master and the other for the NGINX instance. You may have to `Refresh` the Azure web page listing the resources in a resource group for the latest changes to be reflected. Select the `Public IP` resource that is attached to your service (it should have the Azure DNS prefix name along with a long random string, without the `master-ip` string), select `Configuration`, add the DNS assigned above (for example, `bdb-test-cluster-0`), click `Save`, and wait for the changes to be applied.

To verify the DNS setting is operational, you can run `nslookup <DNS name added in Azure configuration>` from your local Linux shell.

This will ensure that when you scale the replica set later, other MongoDB members in the replica set can reach this instance.

5.7.6 Step 6: Start the MongoDB Kubernetes Service

- This configuration is located in the file `mongodb/mongo-svc.yaml`.
- Set the `metadata.name` and `metadata.labels.name` to the value set in `mdb-instance-name` in the ConfigMap above.
- Set the `spec.selector.app` to the value set in `mdb-instance-name` in the ConfigMap followed by `-ss`. For example, if the value set in the `mdb-instance-name` is `mdb-instance-0`, set the `spec.selector.app` to `mdb-instance-0-ss`.
- Set `ports[0].port` and `ports[0].targetPort` to the value set in the `mongodb-backend-port` in the ConfigMap above. This is the `mdb-port` in the file which specifies where MongoDB listens for API requests.
- Start the Kubernetes Service:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f mongodb/mongo-svc.yaml
```

5.7.7 Step 7: Start the BigchainDB Kubernetes Service

- This configuration is located in the file `bigchaindb/bigchaindb-svc.yaml`.
- Set the `metadata.name` and `metadata.labels.name` to the value set in `bdb-instance-name` in the ConfigMap above.
- Set the `spec.selector.app` to the value set in `bdb-instance-name` in the ConfigMap followed by `-dep`. For example, if the value set in the `bdb-instance-name` is `bdb-instance-0`, set the `spec.selector.app` to `bdb-instance-0-dep`.
- Set `ports[0].port` and `ports[0].targetPort` to the value set in the `bigchaindb-api-port` in the ConfigMap above. This is the `bdb-api-port` in the file which specifies where BigchainDB listens for HTTP API requests.
- Set `ports[1].port` and `ports[1].targetPort` to the value set in the `bigchaindb-ws-port` in the ConfigMap above. This is the `bdb-ws-port` in the file which specifies where BigchainDB listens for Websocket connections.
- Start the Kubernetes Service:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f bigchaindb/
↪bigchaindb-svc.yaml
```

5.7.8 Step 8: Start the OpenResty Kubernetes Service

- This configuration is located in the file `nginx-openresty/nginx-openresty-svc.yaml`.
- Set the `metadata.name` and `metadata.labels.name` to the value set in `openresty-instance-name` in the ConfigMap above.
- Set the `spec.selector.app` to the value set in `openresty-instance-name` in the ConfigMap followed by `-dep`. For example, if the value set in the `openresty-instance-name` is `openresty-instance-0`, set the `spec.selector.app` to `openresty-instance-0-dep`.
- Start the Kubernetes Service:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f nginx-openresty/nginx-
↪openresty-svc.yaml
```

5.7.9 Step 9: Start the NGINX Kubernetes Deployment

- NGINX is used as a proxy to OpenResty, BigchainDB and MongoDB instances in the node. It proxies HTTP/HTTPS requests on the `cluster-frontend-port` to the corresponding OpenResty or BigchainDB backend, and TCP connections on `mongodb-frontend-port` to the MongoDB backend.
- As in step 4, you have the option to use vanilla NGINX without HTTPS or NGINX with HTTPS support.

Step 9.1: Vanilla NGINX

- This configuration is located in the file `nginx-http/nginx-http-dep.yaml`.
- Set the `metadata.name` and `spec.template.metadata.labels.app` to the value set in `ngx-instance-name` in the ConfigMap followed by a `-dep`. For example, if the value set in the `ngx-instance-name` is `ngx-http-instance-0`, set the fields to `ngx-http-instance-0-dep`.
- Set the ports to be exposed from the pod in the `spec.containers[0].ports` section. We currently expose 3 ports - `mongodb-frontend-port`, `cluster-frontend-port` and `cluster-health-check-port`. Set them to the values specified in the ConfigMap.
- The configuration uses the following values set in the ConfigMap:
  - `cluster-frontend-port`
  - `cluster-health-check-port`
  - `cluster-dns-server-ip`
  - `mongodb-frontend-port`
  - `ngx-mdb-instance-name`
  - `mongodb-backend-port`
  - `ngx-bdb-instance-name`
  - `bigchaindb-api-port`

  - `bigchaindb-ws-port`

- Start the Kubernetes Deployment:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f nginx-http/nginx-
↪http-dep.yaml
```

Step 9.2: NGINX with HTTPS

- This configuration is located in the file `nginx-https/nginx-https-dep.yaml`.
- Set the `metadata.name` and `spec.template.metadata.labels.app` to the value set in `ngx-instance-name` in the ConfigMap followed by a `-dep`. For example, if the value set in the `ngx-instance-name` is `ngx-https-instance-0`, set the fields to `ngx-https-instance-0-dep`.
- Set the ports to be exposed from the pod in the `spec.containers[0].ports` section. We currently expose 3 ports - `mongodb-frontend-port`, `cluster-frontend-port` and `cluster-health-check-port`. Set them to the values specified in the ConfigMap.
- The configuration uses the following values set in the ConfigMap:
  - `cluster-frontend-port`
  - `cluster-health-check-port`
  - `cluster-fqdn`
  - `cluster-dns-server-ip`
  - `mongodb-frontend-port`
  - `ngx-mdb-instance-name`
  - `mongodb-backend-port`
  - `openresty-backend-port`
  - `ngx-openresty-instance-name`
  - `ngx-bdb-instance-name`
  - `bigchaindb-api-port`
  - `bigchaindb-ws-port`
- The configuration uses the following values set in the Secret:
  - `https-certs`
- Start the Kubernetes Deployment:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f nginx-https/nginx-
↪https-dep.yaml
```

5.7.10 Step 10: Create Kubernetes Storage Classes for MongoDB

MongoDB needs somewhere to store its data persistently, outside the container where MongoDB is running. Our MongoDB Docker container (based on the official MongoDB Docker container) exports two volume mounts with correct permissions from inside the container:

- The directory where the mongod instance stores its data: `/data/db`. There's more explanation in the MongoDB docs about storage.dbpath.
- The directory where the mongodb instance stores the metadata for a sharded cluster: `/data/configdb/`. There's more explanation in the MongoDB docs about sharding.configDB.

Explaining how Kubernetes handles persistent volumes, and the associated terminology, is beyond the scope of this documentation; see the Kubernetes docs about persistent volumes.

The first thing to do is create the Kubernetes storage classes.

Set up Storage Classes in Azure. First, you need an Azure storage account. If you deployed your Kubernetes cluster on Azure using the Azure CLI 2.0 (as per *our template*), then the *az acs create* command already created a storage account in the same location and resource group as your Kubernetes cluster. Both should have the same "storage account SKU": `Standard_LRS`. Standard storage is lower-cost and lower-performance. It uses hard disk drives (HDD). LRS means locally-redundant storage: three replicas in the same data center. Premium storage is higher-cost and higher-performance. It uses solid state drives (SSD). You can create a storage account for Premium storage and associate it with your Azure resource group. For future reference, the command to create a storage account is az storage account create.

Note: Please refer to Azure documentation for the list of VMs that are supported by Premium Storage.

The Kubernetes template for configuration of Storage Class is located in the file `mongodb/mongo-sc.yaml`.

You may have to update the `parameters.location` field in the file to specify the location you are using in Azure.

If you want to use a custom storage account with the Storage Class, you can also update *parameters.storageAccount* and provide the Azure storage account name.

Create the required storage classes using:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f mongodb/mongo-sc.yaml
```

You can check if it worked using `kubectl get storageclasses`.

5.7.11 Step 11: Create Kubernetes Persistent Volume Claims

Next, you will create two PersistentVolumeClaim objects `mongo-db-claim` and `mongo-configdb-claim`.

This configuration is located in the file `mongodb/mongo-pvc.yaml`.

Note how there's no explicit mention of Azure, AWS or whatever. `ReadWriteOnce` (RWO) means the volume can be mounted as read-write by a single Kubernetes node. (`ReadWriteOnce` is the *only* access mode supported by AzureDisk.) `storage: 20Gi` means the volume has a size of 20 gibibytes.

You may want to update the `spec.resources.requests.storage` field in both the files to specify a different disk size.

Create the required Persistent Volume Claims using:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f mongodb/mongo-pvc.yaml
```

You can check its status using: `kubectl get pvc -w`

Initially, the status of persistent volume claims might be "Pending" but it should become "Bound" fairly quickly.

Note: The default Reclaim Policy for dynamically created persistent volumes is `Delete` which means the PV and its associated Azure storage resource will be automatically deleted on deletion of PVC or PV. In order to prevent this

from happening do the following steps to change default reclaim policy of dyanmically created PVs from `Delete` to `Retain`

- Run the following command to list existing PVs

```
$ kubectl --context k8s-bdb-test-cluster-0 get pv
```

- Run the following command to update a PV's reclaim policy to <Retain>

```
$ kubectl --context k8s-bdb-test-cluster-0 patch pv <pv-name> -p '{"spec":{
↪"persistentVolumeReclaimPolicy":"Retain"}}'
```

For notes on recreating a private volume form a released Azure disk resource consult *the page about cluster troubleshooting*.

5.7.12 Step 12: Start a Kubernetes StatefulSet for MongoDB

- This configuration is located in the file `mongodb/mongo-ss.yaml`.
- Set the `spec.serviceName` to the value set in `mdb-instance-name` in the ConfigMap. For example, if the value set in the `mdb-instance-name` is `mdb-instance-0`, set the field to `mdb-instance-0`.
- Set `metadata.name`, `spec.template.metadata.name` and `spec.template.metadata.labels.app` to the value set in `mdb-instance-name` in the ConfigMap, followed by `-ss`. For example, if the value set in the `mdb-instance-name` is `mdb-instance-0`, set the fields to the value `mdb-insance-0-ss`.
- Note how the MongoDB container uses the `mongo-db-claim` and the `mongo-configdb-claim` PersistentVolumeClaims for its `/data/db` and `/data/configdb` directories (mount paths).
- Note also that we use the pod's `securityContext.capabilities.add` specification to add the `FOWNER` capability to the container. That is because the MongoDB container has the user `mongodb`, with uid `999` and group `mongodb`, with gid `999`. When this container runs on a host with a mounted disk, the writes fail when there is no user with uid `999`. To avoid this, we use the Docker feature of `--cap-add=FOWNER`. This bypasses the uid and gid permission checks during writes and allows data to be persisted to disk. Refer to the Docker docs for details.
- As we gain more experience running MongoDB in testing and production, we will tweak the `resources.limits.cpu` and `resources.limits.memory`.
- Set the ports to be exposed from the pod in the `spec.containers[0].ports` section. We currently only expose the MongoDB backend port. Set it to the value specified for `mongodb-backend-port` in the ConfigMap.
- The configuration uses the following values set in the ConfigMap:
  - `mdb-instance-name`
  - `mongodb-replicaset-name`
  - `mongodb-backend-port`
- The configuration uses the following values set in the Secret:
  - `mdb-certs`
  - `ca-auth`

- **Optional**: You can change the value for `STORAGE_ENGINE_CACHE_SIZE` in the ConfigMap `storage-engine-cache-size`, for more information regarding this configuration, please consult the MongoDB Official Documentation.
- **Optional**: If you are not using the **Standard_D2_v2** virtual machines for Kubernetes agents as per the guide, please update the `resources` for `mongo-ss`. We suggest allocating `memory` using the following scheme for a MongoDB StatefulSet:

```
memory = (Total_Memory_Agent_VM_GB - 2GB)
STORAGE_ENGINE_CACHE_SIZE = memory / 2
```

- Create the MongoDB StatefulSet using:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f mongodb/mongo-ss.yaml
```

- It might take up to 10 minutes for the disks, specified in the Persistent Volume Claims above, to be created and attached to the pod. The UI might show that the pod has errored with the message "timeout expired waiting for volumes to attach/mount". Use the CLI below to check the status of the pod in this case, instead of the UI. This happens due to a bug in Azure ACS.

```
$ kubectl --context k8s-bdb-test-cluster-0 get pods -w
```

5.7.13 Step 13: Configure Users and Access Control for MongoDB

- In this step, you will create a user on MongoDB with authorization to create more users and assign roles to them. Note: You need to do this only when setting up the first MongoDB node of the cluster.
- Find out the name of your MongoDB pod by reading the output of the `kubectl ... get pods` command at the end of the last step. It should be something like `mdb-instance-0-ss-0`.
- Log in to the MongoDB pod using:

```
$ kubectl --context k8s-bdb-test-cluster-0 exec -it <name of your MongoDB pod>␣
↪bash
```

- Open a mongo shell using the certificates already present at `/etc/mongod/ssl/`

```
$ mongo --host localhost --port 27017 --verbose --ssl \
  --sslCAFile /etc/mongod/ca/ca.pem \
  --sslPEMKeyFile /etc/mongod/ssl/mdb-instance.pem
```

- Initialize the replica set using:

```
> rs.initiate( {
    _id : "bigchain-rs",
    members: [ {
      _id : 0,
      host  :"<hostname>:27017"
    } ]
  } )
```

  The `hostname` in this case will be the value set in `mdb-instance-name` in the ConfigMap. For example, if the value set in the `mdb-instance-name` is `mdb-instance-0`, set the `hostname` above to the value `mdb-instance-0`.
- The instance should be voted as the `PRIMARY` in the replica set (since this is the only instance in the replica set till now). This can be observed from the mongo shell prompt, which will read `PRIMARY>`.

- Create a user `adminUser` on the `admin` database with the authorization to create other users. This will only work the first time you log in to the mongo shell. For further details, see localhost exception in MongoDB.

```
PRIMARY> use admin
PRIMARY> db.createUser( {
            user: "adminUser",
            pwd: "superstrongpassword",
            roles: [ { role: "userAdminAnyDatabase", db: "admin" },
                     { role: "clusterManager", db: "admin"} ]
          } )
```

- Exit and restart the mongo shell using the above command. Authenticate as the `adminUser` we created earlier:

```
PRIMARY> use admin
PRIMARY> db.auth("adminUser", "superstrongpassword")
```

`db.auth()` returns 0 when authentication is not successful, and 1 when successful.

- We need to specify the user name *as seen in the certificate* issued to the BigchainDB instance in order to authenticate correctly. Use the following `openssl` command to extract the user name from the certificate:

```
$ openssl x509 -in <path to the bigchaindb certificate> \
  -inform PEM -subject -nameopt RFC2253
```

You should see an output line that resembles:

```
subject= emailAddress=dev@bigchaindb.com,CN=test-bdb-ssl,OU=BigchainDB-Instance,
↪O=BigchainDB GmbH,L=Berlin,ST=Berlin,C=DE
```

The `subject` line states the complete user name we need to use for creating the user on the mongo shell as follows:

```
PRIMARY> db.getSiblingDB("$external").runCommand( {
            createUser: 'emailAddress=dev@bigchaindb.com,CN=test-bdb-ssl,
↪OU=BigchainDB-Instance,O=BigchainDB GmbH,L=Berlin,ST=Berlin,C=DE',
            writeConcern: { w: 'majority' , wtimeout: 5000 },
            roles: [
              { role: 'clusterAdmin', db: 'admin' },
              { role: 'readWriteAnyDatabase', db: 'admin' }
            ]
          } )
```

- You can similarly create users for MongoDB Monitoring Agent and MongoDB Backup Agent. For example:

```
PRIMARY> db.getSiblingDB("$external").runCommand( {
            createUser: 'emailAddress=dev@bigchaindb.com,CN=test-mdb-mon-ssl,
↪OU=MongoDB-Mon-Instance,O=BigchainDB GmbH,L=Berlin,ST=Berlin,C=DE',
            writeConcern: { w: 'majority' , wtimeout: 5000 },
            roles: [
              { role: 'clusterMonitor', db: 'admin' }
            ]
          } )

PRIMARY> db.getSiblingDB("$external").runCommand( {
            createUser: 'emailAddress=dev@bigchaindb.com,CN=test-mdb-bak-ssl,
↪OU=MongoDB-Bak-Instance,O=BigchainDB GmbH,L=Berlin,ST=Berlin,C=DE',
            writeConcern: { w: 'majority' , wtimeout: 5000 },
            roles: [
              { role: 'backup',     db: 'admin' }
```

```
            ]
          } )
```

5.7.14 Step 14: Start a Kubernetes Deployment for MongoDB Monitoring Agent

- This configuration is located in the file `mongodb-monitoring-agent/mongo-mon-dep.yaml`.
- Set `metadata.name`, `spec.template.metadata.name` and `spec.template.metadata.labels.app` to the value set in `mdb-mon-instance-name` in the ConfigMap, followed by `-dep`. For example, if the value set in the `mdb-mon-instance-name` is `mdb-mon-instance-0`, set the fields to the value `mdb-mon-instance-0-dep`.
- The configuration uses the following values set in the Secret:
  - `mdb-mon-certs`
  - `ca-auth`
  - `cloud-manager-credentials`
- Start the Kubernetes Deployment using:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f mongodb-monitoring-agent/
↪mongo-mon-dep.yaml
```

5.7.15 Step 15: Start a Kubernetes Deployment for MongoDB Backup Agent

- This configuration is located in the file `mongodb-backup-agent/mongo-backup-dep.yaml`.
- Set `metadata.name`, `spec.template.metadata.name` and `spec.template.metadata.labels.app` to the value set in `mdb-bak-instance-name` in the ConfigMap, followed by `-dep`. For example, if the value set in the `mdb-bak-instance-name` is `mdb-bak-instance-0`, set the fields to the value `mdb-bak-instance-0-dep`.
- The configuration uses the following values set in the Secret:
  - `mdb-bak-certs`
  - `ca-auth`
  - `cloud-manager-credentials`
- Start the Kubernetes Deployment using:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f mongodb-backup-agent/mongo-
↪backup-dep.yaml
```

5.7.16 Step 16: Start a Kubernetes Deployment for BigchainDB

- This configuration is located in the file `bigchaindb/bigchaindb-dep.yaml`.
- Set `metadata.name` and `spec.template.metadata.labels.app` to the value set in `bdb-instance-name` in the ConfigMap, followed by `-dep`. For example, if the value set in the `bdb-instance-name` is `bdb-instance-0`, set the fields to the value `bdb-insance-0-dep`.

- Set the value of `BIGCHAINDB_KEYPAIR_PRIVATE` (not base64-encoded). (In the future, we'd like to pull the BigchainDB private key from the Secret named `bdb-private-key`, but a Secret can only be mounted as a file, so BigchainDB Server would have to be modified to look for it in a file.)
- As we gain more experience running BigchainDB in testing and production, we will tweak the `resources.limits` values for CPU and memory, and as richer monitoring and probing becomes available in BigchainDB, we will tweak the `livenessProbe` and `readinessProbe` parameters.
- Set the ports to be exposed from the pod in the `spec.containers[0].ports` section. We currently expose 2 ports - `bigchaindb-api-port` and `bigchaindb-ws-port`. Set them to the values specified in the ConfigMap.
- The configuration uses the following values set in the ConfigMap:
  - `mdb-instance-name`
  - `mongodb-backend-port`
  - `mongodb-replicaset-name`
  - `bigchaindb-database-name`
  - `bigchaindb-server-bind`
  - `bigchaindb-ws-interface`
  - `cluster-fqdn`
  - `bigchaindb-ws-port`
  - `cluster-frontend-port`
  - `bigchaindb-wsserver-advertised-scheme`
  - `bdb-public-key`
  - `bigchaindb-backlog-reassign-delay`
  - `bigchaindb-database-maxtries`
  - `bigchaindb-database-connection-timeout`
  - `bigchaindb-log-level`
  - `bdb-user`
- The configuration uses the following values set in the Secret:
  - `bdb-certs`
  - `ca-auth`
- Create the BigchainDB Deployment using:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f bigchaindb/bigchaindb-dep.yaml
```

- You can check its status using the command `kubectl get deployments -w`

5.7.17 Step 17: Start a Kubernetes Deployment for OpenResty

- This configuration is located in the file `nginx-openresty/nginx-openresty-dep.yaml`.
- Set `metadata.name` and `spec.template.metadata.labels.app` to the value set in `openresty-instance-name` in the ConfigMap, followed by `-dep`. For example, if the value

set in the `openresty-instance-name` is `openresty-instance-0`, set the fields to the value `openresty-instance-0-dep`.

- Set the port to be exposed from the pod in the `spec.containers[0].ports` section. We currently expose the port at which OpenResty is listening for requests, `openresty-backend-port` in the above ConfigMap.
- The configuration uses the following values set in the Secret:
  - `threescale-credentials`
- The configuration uses the following values set in the ConfigMap:
  - `cluster-dns-server-ip`
  - `openresty-backend-port`
  - `ngx-bdb-instance-name`
  - `bigchaindb-api-port`
- Create the OpenResty Deployment using:

```
$ kubectl --context k8s-bdb-test-cluster-0 apply -f nginx-openresty/nginx-
↪openresty-dep.yaml
```

- You can check its status using the command `kubectl get deployments -w`

5.7.18 Step 18: Configure the MongoDB Cloud Manager

Refer to the *documentation* for details on how to configure the MongoDB Cloud Manager to enable monitoring and backup.

5.7.19 Step 19: Verify the BigchainDB Node Setup

Step 19.1: Testing Internally

To test the setup of your BigchainDB node, you could use a Docker container that provides utilities like `nslookup`, `curl` and `dig`. For example, you could use a container based on our bigchaindb/toolbox image. (The corresponding Dockerfile is in the `bigchaindb/bigchaindb` repository on GitHub.) You can use it as below to get started immediately:

```
$ kubectl --context k8s-bdb-test-cluster-0 \
   run -it toolbox \
   --image bigchaindb/toolbox \
   --image-pull-policy=Always \
   --restart=Never --rm
```

It will drop you to the shell prompt.

To test the MongoDB instance:

```
$ nslookup mdb-instance-0

$ dig +noall +answer _mdb-port._tcp.mdb-instance-0.default.svc.cluster.local SRV

$ curl -X GET http://mdb-instance-0:27017
```

The `nslookup` command should output the configured IP address of the service (in the cluster). The `dig` command should return the configured port numbers. The `curl` command tests the availability of the service.

To test the BigchainDB instance:

```
$ nslookup bdb-instance-0

$ dig +noall +answer _bdb-api-port._tcp.bdb-instance-0.default.svc.cluster.local SRV

$ dig +noall +answer _bdb-ws-port._tcp.bdb-instance-0.default.svc.cluster.local SRV

$ curl -X GET http://bdb-instance-0:9984

$ wsc -er ws://bdb-instance-0:9985/api/v1/streams/valid_transactions
```

To test the OpenResty instance:

```
$ nslookup openresty-instance-0

$ dig +noall +answer _openresty-svc-port._tcp.openresty-instance-0.default.svc.
↪cluster.local SRV
```

To verify if OpenResty instance forwards the requests properly, send a `POST` transaction to OpenResty at post `80` and check the response from the backend BigchainDB instance.

To test the vanilla NGINX instance:

```
$ nslookup ngx-http-instance-0

$ dig +noall +answer _public-cluster-port._tcp.ngx-http-instance-0.default.svc.
↪cluster.local SRV

$ dig +noall +answer _public-health-check-port._tcp.ngx-http-instance-0.default.svc.
↪cluster.local SRV

$ wsc -er ws://ngx-http-instance-0/api/v1/streams/valid_transactions

$ curl -X GET http://ngx-http-instance-0:27017
```

The above curl command should result in the response `It looks like you are trying to access MongoDB over HTTP on the native driver port.`

To test the NGINX instance with HTTPS and 3scale integration:

```
$ nslookup ngx-instance-0

$ dig +noall +answer _public-secure-cluster-port._tcp.ngx-instance-0.default.svc.
↪cluster.local SRV

$ dig +noall +answer _public-mdb-port._tcp.ngx-instance-0.default.svc.cluster.local␣
↪SRV

$ dig +noall +answer _public-insecure-cluster-port._tcp.ngx-instance-0.default.svc.
↪cluster.local SRV

$ wsc -er wss://<cluster-fqdn>/api/v1/streams/valid_transactions

$ curl -X GET http://<cluster-fqdn>:27017
```

The above curl command should result in the response `It looks like you are trying to access MongoDB over HTTP on the native driver port.`

Step 19.2: Testing Externally

Check the MongoDB monitoring and backup agent on the MongoDB Cloud Manager portal to verify they are working fine.

If you are using the NGINX with HTTP support, accessing the URL `http://<DNS/IP of your exposed BigchainDB service endpoint>:cluster-frontend-port` on your browser should result in a JSON response that shows the BigchainDB server version, among other things. If you are using the NGINX with HTTPS support, use `https` instead of `http` above.

Use the Python Driver to send some transactions to the BigchainDB node and verify that your node or cluster works as expected.

5.8 How to Configure a BigchainDB Node

This page outlines the steps to set a bunch of configuration settings in your BigchainDB node. They are pushed to the Kubernetes cluster in two files, named `config-map.yaml` (a set of ConfigMaps) and `secret.yaml` (a set of Secrets). They are stored in the Kubernetes cluster's key-value store (etcd).

Make sure you did all the things listed in the section titled *Things Each Node Operator Must Do* (including generation of all the SSL certificates needed for MongoDB auth).

5.8.1 Edit config-map.yaml

Make a copy of the file `k8s/configuration/config-map.yaml` and edit the data values in the various ConfigMaps. That file already contains many comments to help you understand each data value, but we make some additional remarks on some of the values below.

Note: None of the data values in `config-map.yaml` need to be base64-encoded. (This is unlike `secret.yaml`, where all data values must be base64-encoded. This is true of all Kubernetes ConfigMaps and Secrets.)

vars.cluster-fqdn

The `cluster-fqdn` field specifies the domain you would have *registered before*.

vars.cluster-frontend-port

The `cluster-frontend-port` field specifies the port on which your cluster will be available to all external clients. It is set to the HTTPS port `443` by default.

vars.cluster-health-check-port

The `cluster-healthcheck-port` is the port number on which health check probes are sent to the main NGINX instance. It is set to `8888` by default.

vars.cluster-dns-server-ip

The `cluster-dns-server-ip` is the IP of the DNS server for a node. We use DNS for service discovery. A Kubernetes deployment always has a DNS server (`kube-dns`) running at 10.0.0.10, and since we use Kubernetes, this is set to `10.0.0.10` by default, which is the default `kube-dns` IP address.

vars.mdb-instance-name and Similar

Your BigchainDB cluster organization should have a standard way of naming instances, so the instances in your BigchainDB node should conform to that standard (i.e. you can't just make up some names). There are some things worth noting about the `mdb-instance-name`:

- MongoDB reads the local `/etc/hosts` file while bootstrapping a replica set to resolve the hostname provided to the `rs.initiate()` command. It needs to ensure that the replica set is being initialized in the same instance where the MongoDB instance is running.
- We use the value in the `mdb-instance-name` field to achieve this.
- This field will be the DNS name of your MongoDB instance, and Kubernetes maps this name to its internal DNS.
- This field will also be used by other MongoDB instances when forming a MongoDB replica set.
- We use `mdb-instance-0`, `mdb-instance-1` and so on in our documentation. Your BigchainDB cluster may use a different naming convention.

vars.ngx-mdb-instance-name and Similar

NGINX needs the FQDN of the servers inside the cluster to be able to forward traffic. The `ngx-openresty-instance-name`, `ngx-mdb-instance-name` and `ngx-bdb-instance-name` are the FQDNs of the OpenResty instance, the MongoDB instance, and the BigchainDB instance in this Kubernetes cluster respectively. In Kubernetes, this is usually the name of the module specified in the corresponding `vars.*-instance-name` followed by the `<namespace name>.svc.cluster.local`. For example, if you run OpenResty in the default Kubernetes namespace, this will be `<vars.openresty-instance-name>.default.svc.cluster.local`

vars.mongodb-frontend-port and vars.mongodb-backend-port

The `mongodb-frontend-port` is the port number on which external clients can access MongoDB. This needs to be restricted to only other MongoDB instances by enabling an authentication mechanism on MongoDB cluster. It is set to `27017` by default.

The `mongodb-backend-port` is the port number on which MongoDB is actually available/listening for requests in your cluster. It is also set to `27017` by default.

vars.openresty-backend-port

The `openresty-backend-port` is the port number on which OpenResty is listening for requests. This is used by the NGINX instance to forward requests destined for the OpenResty instance to the right port. This is also used by OpenResty instance to bind to the correct port to receive requests from NGINX instance. It is set to `80` by default.

vars.bigchaindb-wsserver-advertised-scheme

The `bigchaindb-wsserver-advertised-scheme` is the protocol used to access the WebSocket API in BigchainDB. This can be set to `wss` or `ws`. It is set to `wss` by default.

vars.bigchaindb-api-port, vars.bigchaindb-ws-port and Similar

The `bigchaindb-api-port` is the port number on which BigchainDB is listening for HTTP requests. Currently set to `9984` by default.

The `bigchaindb-ws-port` is the port number on which BigchainDB is listening for Websocket requests. Currently set to `9985` by default.

There's another *page with a complete listing of all the BigchainDB Server configuration settings*.

bdb-config.bdb-keyring

This lists the BigchainDB public keys of all *other* nodes in your BigchainDB cluster (not including the public key of your BigchainDB node). Cases:

- If you're deploying the first node in the cluster, the value should be `""` (an empty string).
- If you're deploying the second node in the cluster, the value should be the BigchainDB public key of the first/original node in the cluster. For example, `"EPQk5i5yYpoUwGVM8VKZRjM8CYxB6j8Lu8i8SG7kGGce"`
- If there are two or more other nodes already in the cluster, the value should be a colon-separated list of the BigchainDB public keys of those other nodes. For example, `"DPjpKbmbPYPKVAuf6VSkqGCf5jzrEh69Ldef6TrLwsEQ:EPQk5i5yYpoUwGVM8VKZRjM8CYxB6j8Lu8i8SG7k`

bdb-config.bdb-user

This is the user name that BigchainDB uses to authenticate itself to the backend MongoDB database.

We need to specify the user name *as seen in the certificate* issued to the BigchainDB instance in order to authenticate correctly. Use the following `openssl` command to extract the user name from the certificate:

```
$ openssl x509 -in <path to the bigchaindb certificate> \
  -inform PEM -subject -nameopt RFC2253
```

You should see an output line that resembles:

```
subject= emailAddress=dev@bigchaindb.com,CN=test-bdb-ssl,OU=BigchainDB-Instance,
↪O=BigchainDB GmbH,L=Berlin,ST=Berlin,C=DE
```

The `subject` line states the complete user name we need to use for this field (`bdb-config.bdb-user`), i.e.

```
emailAddress=dev@bigchaindb.com,CN=test-bdb-ssl,OU=BigchainDB-Instance,O=BigchainDB␣
↪GmbH,L=Berlin,ST=Berlin,C=DE
```

5.8.2 Edit secret.yaml

Make a copy of the file `k8s/configuration/secret.yaml` and edit the data values in the various Secrets. That file includes many comments to explain the required values. **In particular, note that all values must be base64-encoded.** There are tips at the top of the file explaining how to convert values into base64-encoded values.

Your BigchainDB node might not need all the Secrets. For example, if you plan to access the BigchainDB API over HTTP, you don't need the `https-certs` Secret. You can delete the Secrets you don't need, or set their data values to `""`.

Note that `ca.pem` is just another name for `ca.crt` (the certificate of your BigchainDB cluster's self-signed CA).

threescale-credentials.*

If you're not using 3scale, you can delete the `threescale-credentials` Secret or leave all the values blank (`""`).

If you *are* using 3scale, get the values for `secret-token`, `service-id`, `version-header` and `service-token` by logging in to 3scale portal using your admin account, click **APIs** and click on **Integration** for the relevant API. Scroll to the bottom of the page and click the small link in the lower right corner, labelled **Download the NGINX Config files**. Unzip it(if it is a `zip` file). Open the `.conf` and the `.lua` file. You should be able to find all the values in those files. You have to be careful because it will have values for **all** your APIs, and some values vary from API to API. The `version-header` is the timestamp in a line that looks like:

```
proxy_set_header  X-3scale-Version "2017-06-28T14:57:34Z";
```

5.8.3 Deploy Your config-map.yaml and secret.yaml

You can deploy your edited `config-map.yaml` and `secret.yaml` files to your Kubernetes cluster using the commands:

```
$ kubectl apply -f config-map.yaml

$ kubectl apply -f secret.yaml
```

5.9 Log Analytics on Azure

This page describes how we use Microsoft Operations Management Suite (OMS) to collect all logs from a Kubernetes cluster, to search those logs, and to set up email alerts based on log messages. The *References* section (below) contains links to more detailed documentation.

There are two steps:

1. Setup: Create a log analytics OMS workspace and a Containers solution under that workspace.
2. Deploy OMS agents to your Kubernetes cluster.

5.9.1 Step 1: Setup

Step 1 can be done the web browser way or the command-line way.

The Web Browser Way

To create a new log analytics OMS workspace:

1. Go to the Azure Portal in your web browser.
2. Click on **More services >** in the lower left corner of the Azure Portal.

3. Type "log analytics" or similar.
4. Select **Log Analytics** from the list of options.
5. Click on **+ Add** to add a new log analytics OMS workspace.
6. Give answers to the questions. You can call the OMS workspace anything, but use the same resource group and location as your Kubernetes cluster. The free option will suffice, but of course you can also use a paid one.

To add a "Containers solution" to that new workspace:

1. In Azure Portal, in the Log Analytics section, click the name of the new workspace
2. Click **OMS Workspace**.
3. Click **OMS Portal**. It should launch the OMS Portal in a new tab.
4. Click the **Solutions Gallery** tile.
5. Click the **Containers** tile.
6. Click **Add**.

The Command-Line Way

We'll assume your Kubernetes cluster has a resource group named:

- `resource_group`

and the workspace we'll create will be named:

- `work_space`

If you feel creative you may replace these names by more interesting ones.

```
$ az group deployment create --debug \
    --resource-group resource_group \
    --name "Microsoft.LogAnalyticsOMS" \
    --template-file log_analytics_oms.json \
    --parameters @log_analytics_oms.parameters.json
```

An example of a simple template file (`--template-file`):

```
{
  "$schema": "http://schema.management.azure.com/schemas/2014-04-01-preview/
↪deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "sku": {
      "type": "String"
    },
    "workspaceName": {
      "type": "String"
    },
    "solutionType": {
      "type": "String"
    },
    "resources": [
      {
        "apiVersion": "2015-03-20",
        "type": "Microsoft.OperationalInsights/workspaces",
        "name": "[parameters('workspaceName')]",
```

```
        "location": "[resourceGroup().location]",
        "properties": {
          "sku": {
            "name": "[parameters('sku')]"
          }
        },
        "resources": [
          {
            "apiVersion": "2015-11-01-preview",
            "location": "[resourceGroup().location]",
            "name": "[Concat(parameters('solutionType'), '(', parameters(
↪'workspaceName'), ')')]",
            "type": "Microsoft.OperationsManagement/solutions",
            "id": "[Concat(resourceGroup().id, '/providers/Microsoft.
↪OperationsManagement/solutions/', parameters('solutionType'), '(', parameters(
↪'workspaceName'), ')')]",
            "dependsOn": [
              "[concat('Microsoft.OperationalInsights/workspaces/', parameters(
↪'workspaceName'))]"
            ],
            "properties": {
              "workspaceResourceId": "[resourceId('Microsoft.OperationalInsights/
↪workspaces/', parameters('workspaceName'))]"
            },
            "plan": {
              "publisher": "Microsoft",
              "product": "[Concat('OMSGallery/', parameters('solutionType'))]",
              "name": "[Concat(parameters('solutionType'), '(', parameters(
↪'workspaceName'), ')')]",
              "promotionCode": ""
            }
          }
        ]
      }
    ]
  }
}
```

An example of the associated parameter file (`--parameters`):

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/
↪deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "sku": {
      "value": "Free"
    },
    "workspaceName": {
      "value": "work_space"
    },
    "solutionType": {
      "value": "Containers"
    }
  }
}
```

5.9.2 Step 2: Deploy the OMS Agents

To deploy an OMS agent, two important pieces of information are needed:

1. workspace id
2. workspace key

You can obtain the workspace id using:

```
$ az resource show \
    --resource-group resource_group
    --resource-type Microsoft.OperationalInsights/workspaces
    --name work_space \
    | grep customerId
"customerId": "12345678-1234-1234-1234-123456789012",
```

Until we figure out a way to obtain the *workspace key* via the command line, you can get it via the OMS Portal. To get to the OMS Portal, go to the Azure Portal and click on:

Resource Groups > (Your k8s cluster's resource group) > Log analytics (OMS) > (Name of the only item listed) > OMS Workspace > OMS Portal

(Let us know if you find a faster way.) Then see Microsoft's instructions to obtain your workspace ID and key (via the OMS Portal).

Once you have the workspace id and key, you can include them in the following YAML file (`oms-daemonset.yaml`):

```
# oms-daemonset.yaml
apiVersion: extensions/v1beta1
kind: DaemonSet
metadata:
  name: omsagent
spec:
  template:
    metadata:
      labels:
        app: omsagent
    spec:
      containers:
      - env:
        - name: WSID
          value: <workspace_id>
        - name: KEY
          value: <workspace_key>
        image: microsoft/oms
        name: omsagent
        ports:
        - containerPort: 25225
          protocol: TCP
        securityContext:
          privileged: true
        volumeMounts:
        - mountPath: /var/run/docker.sock
          name: docker-sock
      volumes:
      - name: docker-sock
        hostPath:
          path: /var/run/docker.sock
```

To deploy the OMS agents (one per Kubernetes node, i.e. one per computer), simply run the following command:

```
$ kubectl create -f oms-daemonset.yaml
```

5.9.3 Search the OMS Logs

OMS should now be getting, storing and indexing all the logs from all the containers in your Kubernetes cluster. You can search the OMS logs from the Azure Portal or the OMS Portal, but at the time of writing, there was more functionality in the OMS Portal (e.g. the ability to create an Alert based on a search).

There are instructions to get to the OMS Portal above. Once you're in the OMS Portal, click on **Log Search** and enter a query. Here are some example queries:

All logging messages containing the strings "critical" or "error" (not case-sensitive):

```
Type=ContainerLog (critical OR error)
```

Note: You can filter the results even more by clicking on things in the left sidebar. For OMS Log Search syntax help, see the Log Analytics search reference.

All logging messages containing the string "error" but not "404":

```
Type=ContainerLog error NOT(404)
```

All logging messages containing the string "critical" but not "CriticalAddonsOnly":

```
Type=ContainerLog critical NOT(CriticalAddonsOnly)
```

All logging messages from containers running the Docker image bigchaindb/nginx_3scale:1.3, containing the string "GET" but not the strings "Go-http-client" or "runscope" (where those exclusions filter out tests by Kubernetes and Runscope):

```
Type=ContainerLog Image="bigchaindb/nginx_3scale:1.3" GET
NOT("Go-http-client") NOT(runscope)
```

Note: We wrote a small Python 3 script to analyze the logs found by the above NGINX search. It's in `k8s/logging-and-monitoring/analyze.py`. The docsting at the top of the script explains how to use it.

5.9.4 Create an Email Alert

Once you're satisfied with an OMS Log Search query string, click the **Alert** icon in the top menu, fill in the form, and click **Save** when you're done.

5.9.5 Some Useful Management Tasks

List workspaces:

```
$ az resource list \
    --resource-group resource_group \
    --resource-type Microsoft.OperationalInsights/workspaces
```

List solutions:

```
$ az resource list \
    --resource-group resource_group \
    --resource-type Microsoft.OperationsManagement/solutions
```

Delete the containers solution:

```
$ az group deployment delete --debug \
    --resource-group resource_group \
    --name Microsoft.ContainersOMS
```

```
$ az resource delete \
    --resource-group resource_group \
    --resource-type Microsoft.OperationsManagement/solutions \
    --name "Containers(work_space)"
```

Delete the workspace:

```
$ az group deployment delete --debug \
    --resource-group resource_group \
    --name Microsoft.LogAnalyticsOMS
```

```
$ az resource delete \
    --resource-group resource_group \
    --resource-type Microsoft.OperationalInsights/workspaces \
    --name work_space
```

5.9.6 References

- Monitor an Azure Container Service cluster with Microsoft Operations Management Suite (OMS)
- Manage Log Analytics using Azure Resource Manager templates
- azure commands for deployments (`az group deployment`)
- Understand the structure and syntax of Azure Resource Manager templates
- Kubernetes DaemonSet

5.10 Configure MongoDB Cloud Manager for Monitoring and Backup

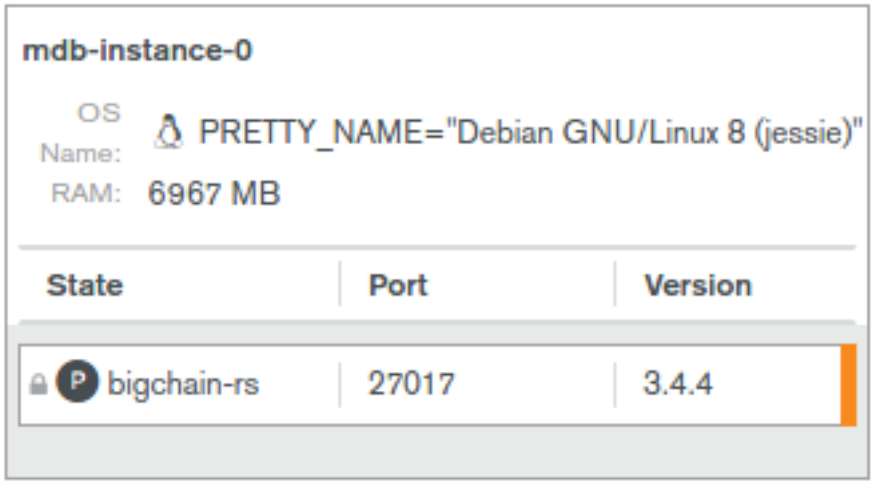
This document details the steps required to configure MongoDB Cloud Manager to enable monitoring and backup of data in a MongoDB Replica Set.

5.10.1 Configure MongoDB Cloud Manager for Monitoring

- Once the Monitoring Agent is up and running, open MongoDB Cloud Manager.
- Click `Login` under `MongoDB Cloud Manager` and log in to the Cloud Manager.
- Select the group from the dropdown box on the page.
- Go to Settings and add a `Preferred Hostnames` entry as a regexp based on the `mdb-instance-name` of the nodes in your cluster. It may take up to 5 mins till this setting takes effect. You may refresh the browser window and verify whether the changes have been saved or not.

For example, for the nodes in a cluster that are named `mdb-instance-0`, `mdb-instance-1` and so on, a regex like `^mdb-instance-[0-9]{1,2}$` is recommended.

- Next, click the `Deployment` tab, and then the `Manage Existing` button.
- On the `Import your deployment for monitoring` page, enter the hostname to be the same as the one set for `mdb-instance-name` in the global ConfigMap for a node. For example, if the `mdb-instance-name` is set to `mdb-instance-0`, enter `mdb-instance-0` as the value in this field.
- Enter the port number as `27017`, with no authentication.
- If you have authentication enabled, select the option to enable authentication and specify the authentication mechanism as per your deployment. The default BigchainDB production deployment currently supports `X.509 Client Certificate` as the authentication mechanism.
- If you have TLS enabled, select the option to enable TLS/SSL for MongoDB connections, and click `Continue`. This should already be selected for you in case you selected `X.509 Client Certificate` above.
- Wait a minute or two for the deployment to be found and then click the `Continue` button again.
- Verify that you see your process on the Cloud Manager UI. It should look something like this:



- Click `Continue`.
- Verify on the UI that data is being sent by the monitoring agent to the Cloud Manager. It may take upto 5 minutes for data to appear on the UI.

5.10.2 Configure MongoDB Cloud Manager for Backup

- Once the Backup Agent is up and running, open MongoDB Cloud Manager.
- Click `Login` under `MongoDB Cloud Manager` and log in to the Cloud Manager.
- Select the group from the dropdown box on the page.
- Click `Backup` tab.
- Hover over the `Status` column of your backup and click `Start` to start the backup.
- Select the replica set on the side pane.
- If you have authentication enabled, select the authentication mechanism as per your deployment. The default BigchainDB production deployment currently supports `X.509 Client Certificate` as the authentication mechanism.

- If you have TLS enabled, select the checkbox `Replica set allows TLS/SSL connections`. This should be selected by default in case you selected `X.509 Client Certificate` as the auth mechanism above.
- Choose the `WiredTiger` storage engine.
- Verify the details of your MongoDB instance and click on `Start`.
- It may take up to 5 minutes for the backup process to start. During this process, the UI will show the status of the backup process.
- Verify that data is being backed up on the UI.

5.11 How to Install & Configure Easy-RSA

We use Easy-RSA version 3, a wrapper over complex `openssl` commands. Easy-RSA is available on GitHub and licensed under GPLv2.

5.11.1 Step 1: Install Easy-RSA Dependencies

The only dependency for Easy-RSA v3 is `openssl`, which is available from the `openssl` package on Ubuntu and other Debian-based operating systems, i.e. you can install it using:

```
sudo apt-get update

sudo apt-get install openssl
```

5.11.2 Step 2: Install Easy-RSA

Make sure you're in the directory where you want Easy-RSA to live, then download it and extract it within that directory:

```
wget https://github.com/OpenVPN/easy-rsa/archive/3.0.1.tar.gz

tar xzvf 3.0.1.tar.gz

rm 3.0.1.tar.gz
```

There should now be a directory named `easy-rsa-3.0.1` in your current directory.

5.11.3 Step 3: Customize the Easy-RSA Configuration

We now create a config file named `vars` by copying the existing `vars.example` file and then editing it. You should change the country, province, city, org and email to the correct values for your organisation. (Note: The country, province, city, org and email are part of the Distinguished Name (DN).) The comments in the file explain what each of the variables mean.

```
cd easy-rsa-3.0.1/easyrsa3

cp vars.example vars

echo 'set_var EASYRSA_DN "org"' >> vars
echo 'set_var EASYRSA_KEY_SIZE 4096' >> vars
```

```
echo 'set_var EASYRSA_REQ_COUNTRY "DE"' >> vars
echo 'set_var EASYRSA_REQ_PROVINCE "Berlin"' >> vars
echo 'set_var EASYRSA_REQ_CITY "Berlin"' >> vars
echo 'set_var EASYRSA_REQ_ORG "BigchainDB GmbH"' >> vars
echo 'set_var EASYRSA_REQ_OU "IT"' >> vars
echo 'set_var EASYRSA_REQ_EMAIL "dev@bigchaindb.com"' >> vars
```

Note: Later, when building a CA or generating a certificate signing request, you will be prompted to enter a value for the OU (or to accept the default). You should change the default OU from `IT` to one of the following, as appropriate: `ROOT-CA`, `MongoDB-Instance`, `BigchainDB-Instance`, `MongoDB-Mon-Instance` or `MongoDB-Backup-Instance`. To understand why, see the MongoDB Manual. There are reminders to do this in the relevant docs.

5.11.4 Step 4: Maybe Edit x509-types/server

Warning: Only do this step if you are setting up a self-signed CA.

Edit the file `x509-types/server` and change `extendedKeyUsage = serverAuth` to `extendedKeyUsage = serverAuth,clientAuth`. See the MongoDB documentation about x.509 authentication to understand why.

5.12 Kubernetes Template: Upgrade all Software in a BigchainDB Node

This page outlines how to upgrade all the software associated with a BigchainDB node running on Kubernetes, including host operating systems, Docker, Kubernetes, and BigchainDB-related software.

5.12.1 Upgrade Host OS, Docker and Kubernetes

Some Kubernetes installation & management systems can do full or partial upgrades of host OSes, Docker, or Kubernetes, e.g. Tectonic, Rancher, and Kubo. Consult the documentation for your system.

Azure Container Service (ACS). On Dec. 15, 2016, a Microsoft employee wrote: "In the coming months we [the Azure Kubernetes team] will be building managed updates in the ACS service." At the time of writing, managed updates were not yet available, but you should check the latest ACS documentation to see what's available now. Also at the time of writing, ACS only supported Ubuntu as the host (master and agent) operating system. You can upgrade Ubuntu and Docker on Azure by SSHing into each of the hosts, as documented on *another page*.

In general, you can SSH to each host in your Kubernetes Cluster to update the OS and Docker.

Note: Once you are in an SSH session with a host, the `docker info` command is a handy way to detemine the host OS (including version) and the Docker version.

When you want to upgrade the software on a Kubernetes node, you should "drain" the node first, i.e. tell Kubernetes to gracefully terminate all pods on the node and mark it as unscheduleable (so no new pods get put on the node during its downtime).

```
kubectl drain $NODENAME
```

There are more details in the Kubernetes docs, including instructions to make the node scheduleable again.

To manually upgrade the host OS, see the docs for that OS.

To manually upgrade Docker, see the Docker docs.

To manually upgrade all Kubernetes software in your Kubernetes cluster, see the Kubernetes docs.

5.12.2 Upgrade BigchainDB-Related Software

We use Kubernetes "Deployments" for NGINX, BigchainDB, and most other BigchainDB-related software. The only exception is MongoDB; we use a Kubernetes StatefulSet for that.

The nice thing about Kubernetes Deployments is that Kubernetes can manage most of the upgrade process. A typical upgrade workflow for a single Deployment would be:

```
$ KUBE_EDITOR=nano kubectl edit deployment/<name of Deployment>
```

The `kubectl edit` command opens the specified editor (nano in the above example), allowing you to edit the specified Deployment *in the Kubernetes cluster*. You can change the version tag on the Docker image, for example. Don't forget to save your edits before exiting the editor. The Kubernetes docs have more information about Deployments (including updating them).

The upgrade story for the MongoDB StatefulSet is *different*. (This is because MongoDB has persistent state, which is stored in some storage associated with a PersistentVolumeClaim.) At the time of writing, StatefulSets were still in beta, and they did not support automated image upgrade (Docker image tag upgrade). We expect that to change. Rather than trying to keep these docs up-to-date, we advise you to check out the current Kubernetes docs about updating containers in StatefulSets.

5.13 Kubernetes Template: Add a BigchainDB Node to an Existing BigchainDB Cluster

This page describes how to deploy a BigchainDB node using Kubernetes, and how to add that node to an existing BigchainDB cluster. It assumes you already have a running Kubernetes cluster where you can deploy the new BigchainDB node.

If you want to deploy the first BigchainDB node in a BigchainDB cluster, or a stand-alone BigchainDB node, then see *the page about that*.

5.13.1 Terminology Used

`existing cluster` will refer to one of the existing Kubernetes clusters hosting one of the existing BigchainDB nodes.

`ctx-1` will refer to the kubectl context of the existing cluster.

`new cluster` will refer to the new Kubernetes cluster that will run a new BigchainDB node (including a BigchainDB instance and a MongoDB instance).

`ctx-2` will refer to the kubectl context of the new cluster.

`new MongoDB instance` will refer to the MongoDB instance in the new cluster.

`existing MongoDB instance` will refer to the MongoDB instance in the existing cluster.

`new BigchainDB instance` will refer to the BigchainDB instance in the new cluster.

`existing BigchainDB instance` will refer to the BigchainDB instance in the existing cluster.

Below, we refer to multiple files by their directory and filename, such as `mongodb/mongo-ext-conn-svc.yaml`. Those files are files in the bigchaindb/bigchaindb repository on GitHub in the `k8s/` directory. Make sure you're getting those files from the appropriate Git branch on GitHub, i.e. the branch for the version of BigchainDB that your BigchainDB cluster is using.

5.13.2 Step 1: Prerequisites

- *List of all the things to be done by each node operator*.
- The public key should be shared offline with the other existing BigchainDB nodes in the existing BigchainDB cluster.
- You will need the public keys of all the existing BigchainDB nodes.
- A new Kubernetes cluster setup with kubectl configured to access it.
- Some familiarity with deploying a BigchainDB node on Kubernetes. See our *other docs about that*.

Note: If you are managing multiple Kubernetes clusters, from your local system, you can run `kubectl config view` to list all the contexts that are available for the local kubectl. To target a specific cluster, add a `--context` flag to the kubectl CLI. For example:

```
$ kubectl --context ctx-1 apply -f example.yaml
$ kubectl --context ctx-2 apply -f example.yaml
$ kubectl --context ctx-1 proxy --port 8001
$ kubectl --context ctx-2 proxy --port 8002
```

5.13.3 Step 2: Configure the BigchainDB Node

See the section on how to *configure your BigchainDB node*.

5.13.4 Step 3: Start the NGINX Service

Please see the following section:

- *Start NGINX service*.

5.13.5 Step 4: Assign DNS Name to the NGINX Public IP

Please see the following section:

- *Assign DNS to NGINX Public IP*.

5.13.6 Step 5: Start the MongoDB Kubernetes Service

Please see the following section:

- *Start the MongoDB Kubernetes Service*.

5.13.7 Step 6: Start the BigchainDB Kubernetes Service

Please see the following section:

- *Start the BigchainDB Kubernetes Service*.

5.13.8 Step 7: Start the OpenResty Kubernetes Service

Please see the following section:

- *Start the OpenResty Kubernetes Service*.

5.13.9 Step 8: Start the NGINX Kubernetes Deployment

Please see the following section:

- *Run NGINX deployment*.

5.13.10 Step 9: Create Kubernetes Storage Classes for MongoDB

Please see the following section:

- *Step 10: Create Kubernetes Storage Classes for MongoDB*.

5.13.11 Step 10: Create Kubernetes Persistent Volume Claims

Please see the following section:

- *Step 11: Create Kubernetes Persistent Volume Claims*.

5.13.12 Step 11: Start a Kubernetes StatefulSet for MongoDB

Please see the following section:

- *Step 12: Start a Kubernetes StatefulSet for MongoDB*.

5.13.13 Step 12: Verify network connectivity between the MongoDB instances

Make sure your MongoDB instances can access each other over the network. *If* you are deploying the new MongoDB node in a different cluster or geographical location using Azure Kubernetes Container Service, you will have to set up networking between the two clusters using Kubernetes Services.

Assuming we have an existing MongoDB instance `mdb-instance-0` residing in Azure data center location `westeurope` and we want to add a new MongoDB instance `mdb-instance-1` located in Azure data center location `eastus` to the existing MongoDB replica set. Unless you already have explicitly set up networking for `mdb-instance-0` to communicate with `mdb-instance-1` and vice versa, we will have to add a Kubernetes Service in each cluster to accomplish this goal in order to set up a MongoDB replica set. It is similar to ensuring that there is a `CNAME` record in the DNS infrastructure to resolve `mdb-instance-X` to the host where it is actually available. We can do this in Kubernetes using a Kubernetes Service of `type ExternalName`.

- This configuration is located in the file `mongodb/mongo-ext-conn-svc.yaml`.

- Set the name of the `metadata.name` to the host name of the MongoDB instance you are trying to connect to. For instance if you are configuring this service on cluster with `mdb-instance-0` then the `metadata.name` will be `mdb-instance-1` and vice versa.
- Set `spec.ports.port[0]` to the `mongodb-backend-port` from the ConfigMap for the other cluster.
- Set `spec.externalName` to the FQDN mapped to NGINX Public IP of the cluster you are trying to connect to. For more information about the FQDN please refer to: *Assign DNS Name to the NGINX Public IP*

Note: This operation needs to be replicated `n-1` times per node for a `n` node cluster, with the respective FQDNs we need to communicate with.

If you are not the system administrator of the cluster, you have to get in touch with the system administrator/s of the other `n-1` clusters and share with them your instance name (`mdb-instance-name` in the ConfigMap) and the FQDN for your node (`cluster-fqdn` in the ConfigMap).

5.13.14 Step 13: Add the New MongoDB Instance to the Existing Replica Set

Note that by `replica set`, we are referring to the MongoDB replica set, not a Kubernetes' `ReplicaSet`.

If you are not the administrator of an existing BigchainDB node, you will have to coordinate offline with an existing administrator so that they can add the new MongoDB instance to the replica set.

Add the new instance of MongoDB from an existing instance by accessing the `mongo` shell and authenticate as the `adminUser` we created for existing MongoDB instance OR contact the admin of the PRIMARY MongoDB node:

```
$ kubectl --context ctx-1 exec -it <existing mongodb-instance-name> bash
$ mongo --host <existing mongodb-instance-name> --port 27017 --verbose --ssl \
  --sslCAFile /etc/mongod/ssl/ca.pem \
  --sslPEMKeyFile /etc/mongod/ssl/mdb-instance.pem

PRIMARY> use admin
PRIMARY> db.auth("adminUser", "superstrongpassword")
```

One can only add members to a replica set from the `PRIMARY` instance. The `mongo` shell prompt should state that this is the primary member in the replica set. If not, then you can use the `rs.status()` command to find out who the primary is and login to the `mongo` shell in the primary.

Run the `rs.add()` command with the FQDN and port number of the other instances:

```
PRIMARY> rs.add("<new mdb-instance-name>:<port>")
```

5.13.15 Step 14: Verify the Replica Set Membership

You can use the `rs.conf()` and the `rs.status()` commands available in the mongo shell to verify the replica set membership.

The new MongoDB instance should be listed in the membership information displayed.

5.13.16 Step 15: Configure Users and Access Control for MongoDB

- Create the users in MongoDB with the appropriate roles assigned to them. This will enable the new BigchainDB instance, new MongoDB Monitoring Agent instance and the new MongoDB Backup Agent instance to function correctly.

- Please refer to *Configure Users and Access Control for MongoDB* to create and configure the new BigchainDB, MongoDB Monitoring Agent and MongoDB Backup Agent users on the cluster.

Note: You will not have to create the MongoDB replica set or create the admin user, as they already exist.

If you do not have access to the `PRIMARY` member of the replica set, you need to get in touch with the administrator who can create the users in the MongoDB cluster.

5.13.17 Step 16: Start a Kubernetes Deployment for MongoDB Monitoring Agent

Please see the following section:

- *Step 14: Start a Kubernetes Deployment for MongoDB Monitoring Agent*.

Note: Every MMS group has only one active Monitoring and Backup Agent and having multiple agents provides high availability and failover, in case one goes down. For more information about Monitoring and Backup Agents please consult the official MongoDB documenation.

5.13.18 Step 17: Start a Kubernetes Deployment for MongoDB Backup Agent

Please see the following section:

- *Step 15: Start a Kubernetes Deployment for MongoDB Backup Agent*.

Note: Every MMS group has only one active Monitoring and Backup Agent and having multiple agents provides high availability and failover, in case one goes down. For more information about Monitoring and Backup Agents please consult the official MongoDB documenation.

5.13.19 Step 18: Start a Kubernetes Deployment for BigchainDB

- Set `metadata.name` and `spec.template.metadata.labels.app` to the value set in `bdb-instance-name` in the ConfigMap, followed by `-dep`. For example, if the value set in the `bdb-instance-name` is `bdb-instance-0`, set the fields to the value `bdb-instance-0-dep`.
- Set the value of `BIGCHAINDB_KEYPAIR_PRIVATE` (not base64-encoded). (In the future, we'd like to pull the BigchainDB private key from the Secret named `bdb-private-key`, but a Secret can only be mounted as a file, so BigchainDB Server would have to be modified to look for it in a file.)
- As we gain more experience running BigchainDB in testing and production, we will tweak the `resources.limits` values for CPU and memory, and as richer monitoring and probing becomes available in BigchainDB, we will tweak the `livenessProbe` and `readinessProbe` parameters.
- Set the ports to be exposed from the pod in the `spec.containers[0].ports` section. We currently expose 2 ports - `bigchaindb-api-port` and `bigchaindb-ws-port`. Set them to the values specified in the ConfigMap.
- Uncomment the env var `BIGCHAINDB_KEYRING`, it will pick up the `:` delimited list of all the public keys in the BigchainDB cluster from the ConfigMap.

Create the required Deployment using:

```
$ kubectl --context ctx-2 apply -f bigchaindb-dep.yaml
```

You can check its status using the command `kubectl --context ctx-2 get deploy -w`

5.13.20 Step 19: Restart the Existing BigchainDB Instance(s)

- Add the public key of the new BigchainDB instance to the ConfigMap `bdb-keyring` variable of all the existing BigchainDB instances. Update all the existing ConfigMap using:

```
$ kubectl --context ctx-1 apply -f configuration/config-map.yaml
```

- Uncomment the `BIGCHAINDB_KEYRING` variable from the `bigchaindb/bigchaindb-dep.yaml` to refer to the keyring updated in the ConfigMap. Update the running BigchainDB instance using:

```
$ kubectl --context ctx-1 delete -f bigchaindb/bigchaindb-dep.yaml
$ kubectl --context ctx-1 apply -f bigchaindb/bigchaindb-dep.yaml
```

See the page titled *How to Configure a BigchainDB Node* for more information about ConfigMap configuration.

You can SSH to an existing BigchainDB instance and run the `bigchaindb show-config` command to check that the keyring is updated.

5.13.21 Step 20: Start a Kubernetes Deployment for OpenResty

Please see the following section:

- *Step 17: Start a Kubernetes Deployment for OpenResty*.

5.13.22 Step 21: Configure the MongoDB Cloud Manager

- MongoDB Cloud Manager auto-detects the members of the replica set and configures the agents to act as a master/slave accordingly.
- You can verify that the new MongoDB instance is detected by the Monitoring and Backup Agent using the Cloud Manager UI.

5.13.23 Step 22: Test Your New BigchainDB Node

- Please refer to the testing steps *here* to verify that your new BigchainDB node is working as expected.

5.14 How to Restore Data Backed On MongoDB Cloud Manager

This page describes how to restore data backed up on MongoDB Cloud Manager by the backup agent when using a single instance MongoDB replica set.

5.14.1 Prerequisites

- You can restore to either new hardware or existing hardware. We cover restoring data to an existing MongoDB Kubernetes StatefulSet using a Kubernetes Persistent Volume Claim below as described *here*.

- If the backup and destination database storage engines or settings do not match, mongod cannot start once the backup is restored.
- If the backup and destination database do not belong to the same MongoDB Cloud Manager group, then the database will start but never initialize properly.
- The backup restore file includes a metadata file, restoreInfo.txt. This file captures the options the database used when the snapshot was taken. The database must be run with the listed options after it has been restored. It contains: 1. Group name 2. Replica Set name 3. Cluster Id (if applicable) 4. Snapshot timestamp (as Timestamp at UTC) 5. Last Oplog applied (as a BSON Timestamp at UTC) 6. MongoDB version 7. Storage engine type 8. mongod startup options used on the database when the snapshot was taken

5.14.2 Step 1: Get the Backup/Archived Data from Cloud Manager

- Log in to the Cloud Manager.
- Select the Group that you want to restore data from.
- Click Backup. Hover over the Status column, click on the `Restore Or Download` button.
- Select the appropriate SNAPSHOT, and click Next.

Note: We currently do not support restoring data using the `POINT IN TIME` and `OPLOG TIMESTAMP` method.

- Select 'Pull via Secure HTTP'. Select the number of times the link can be used to download data in the dropdown box. We select `Once`. Select the link expiration time - the time till the download link is active. We usually select `1 hour`.
- Check for the email from MongoDB.

Note: This can take some time as the Cloud Manager needs to prepare an archive of the backed up data.

- Once you receive the email, click on the link to open the `restore jobs page`. Follow the instructions to download the backup data.

Note: You will be shown a link to download the back up archive. You can either click on the `Download` button to download it using the browser. Under rare circumstances, the download is interrupted and errors out; I have no idea why. An alternative is to copy the download link and use the `wget` tool on Linux systems to download the data.

5.14.3 Step 2: Copy the archive to the MongoDB Instance

- Once you have the archive, you can copy it to the MongoDB instance running on a Kubernetes cluster using something similar to:

```
 $ kubectl --context ctx-1 cp bigchain-rs-XXXX.tar.gz mdb-instance-name:/

where ``bigchain-rs-XXXX.tar.gz`` is the archive downloaded from Cloud
Manager, and ``mdb-instance-name`` is the name of your MongoDB instance.
```

5.14.4 Step 3: Prepare the MongoDB Instance for Restore

- Log in to the MongoDB instance using something like:

```
$ kubectl --context ctx-1 exec -it mdb-instance-name bash
```

- Extract the archive that we have copied to the instance at the proper location using:

```
$ mv /bigchain-rs-XXXX.tar.gz /data/db

$ cd /data/db

$ tar xzvf bigchain-rs-XXXX.tar.gz
```

- Rename the directories on the disk, so that MongoDB can find the correct data after we restart it.
- The current database will be located in the `/data/db/main` directory. We simply rename the old directory to `/data/db/main.BAK` and rename the backup directory `bigchain-rs-XXXX` to `main`.

```
$ mv main main.BAK

$ mv bigchain-rs-XXXX main
```

Note: Ensure that there are no connections to MongoDB from any client, in our case, BigchainDB. This can be done in multiple ways - iptable rules, shutting down BigchainDB, stop sending any transactions to BigchainDB, etc. The simplest way to do it is to stop the MongoDB Kubernetes Service. BigchainDB has a retry mechanism built in, and it will keep trying to connect to MongoDB backend repeatedly till it succeeds.

5.14.5 Step 4: Restart the MongoDB Instance

- This can be achieved using something like:

```
$ kubectl --context ctx-1 delete -f k8s/mongo/mongo-ss.yaml

$ kubectl --context ctx-1 apply -f  k8s/mongo/mongo-ss.yaml
```

5.15 Walkthrough: Deploy a Kubernetes Cluster on Azure using Tectonic by CoreOS

A BigchainDB node can be run inside a Kubernetes cluster. This page describes one way to deploy a Kubernetes cluster on Azure using Tectonic. Tectonic helps in easier cluster management of Kubernetes clusters.

If you would rather use Azure Container Service to manage Kubernetes Clusters, please read *our guide for that*.

5.15.1 Step 1: Prerequisites for Deploying Tectonic Cluster

Get an Azure account. Refer to *this step in our docs*.

Create an SSH Key pair for the new Tectonic cluster. Refer to *this step in our docs*.

5.15.2 Step 2: Get a Tectonic Subscription

CoreOS offers Tectonic for free for up to 10 nodes.

Sign up for an account here if you do not have one already and get a license for 10 nodes.

Login to your account, go to Overview > Your Account and save the `CoreOS License` and the `Pull Secret` to your local machine.

5.15.3 Step 3: Deploy the cluster on Azure

The latest instructions for deployment can be found here.

The following points suggests some customizations for a BigchainDB deployment when following the steps above:

1. Set the `CLUSTER` variable to the name of the cluster. Also note that the cluster will be deployed in a resource group named `tectonic-cluster-CLUSTER`.
2. Set the `tectonic_base_domain` to `""` if you want to use Azure managed DNS. You will be assigned a `cloudapp.azure.com` sub-domain by default and you can skip the `Configuring Azure DNS` section from the Tectonic installation guide.
3. Set the `tectonic_cl_channel` to `"stable"` unless you want to experiment or test with the latest release.
4. Set the `tectonic_cluster_name` to the `CLUSTER` variable defined in the step above.
5. Set the `tectonic_license_path` and `tectonic_pull_secret_path` to the location where you have stored the `tectonic-license.txt` and the `config.json` files downloaded in the previous step.
6. Set the `tectonic_etcd_count` to `"3"`, so that you have a multi-node etcd cluster that can tolerate a single node failure.
7. Set the `tectonic_etcd_tls_enabled` to `"true"` as this will enable TLS connectivity between the etcd nodes and their clients.
8. Set the `tectonic_master_count` to `"3"` so that you cane tolerate a single master failure.
9. Set the `tectonic_worker_count` to `"2"`.
10. Set the `tectonic_azure_location` to `"westeurope"` if you want to host the cluster in Azure's `westeurope` datacenter.
11. Set the `tectonic_azure_ssh_key` to the path of the public key created in the previous step.
12. We recommend setting up or using a CA(Certificate Authority) to generate Tectonic Console's server certificate(s) and adding it to your trusted authorities on the client side, accessing the Tectonic Console i.e. Browser. If you already have a CA(self-signed or otherwise), Set the `tectonic_ca_cert` and `tectonic_ca_key` configurations with the content of PEM-encoded certificate and key files, respectively. For more information about, how to set up a self-signed CA, Please refer to *How to Set up self-signed CA*.
13. Note that the `tectonic_azure_client_secret` is the same as the `ARM_CLIENT_SECRET`.
14. Note that the URL for the Tectonic console using these settings will be the cluster name set in the configutation file, the datacenter name and `cloudapp.azure.com`. For example, if you named your cluster as `test-cluster` and specified the datacenter as `westeurope`, the Tectonic console will be available at `test-cluster.westeurope.cloudapp.azure.com`.
15. Note that, if you do not specify `tectonic_ca_cert`, a CA certificate will be generated automatically and you will encounter the untrusted certificate message on your client(Browser), when accessing the Tectonic Console.

5.15.4 Step 4: Configure kubectl

1. Refer to this tutorial for instructions on how to download the kubectl configuration files for your cluster.
2. Set the `KUBECONFIG` environment variable to make `kubectl` use the new config file along with the existing configuration.

```
$ export KUBECONFIG=$HOME/.kube/config:/path/to/config/kubectl-config

# OR to only use the new configuration, try

$ export KUBECONFIG=/path/to/config/kubectl-config
```

Next, you can *run a BigchainDB node on your new Kubernetes cluster*.

5.15.5 Tectonic References

1. https://coreos.com/tectonic/docs/latest/tutorials/azure/install.html
2. https://coreos.com/tectonic/docs/latest/troubleshooting/installer-terraform.html
3. https://coreos.com/tectonic/docs/latest/tutorials/azure/first-app.html

5.16 Cluster Troubleshooting

This page describes some basic issues we have faced while deploying and operating the cluster.

5.16.1 1. MongoDB Restarts

We define the following in the `mongo-ss.yaml` file:

```
resources:
  limits:
    cpu: 200m
    memory: 5G
```

When the MongoDB cache occupies a memory greater than 5GB, it is terminated by the `kubelet`. This can usually be verified by logging in to the worker node running MongoDB container and looking at the syslog (the `journalctl` command should usually work).

This issue is resolved in PR #1757.

5.16.2 2. 502 Bad Gateway Error on Runscope Tests

It means that NGINX could not find the appropriate backed to forward the requests to. This typically happens when:

1. MongoDB goes down (as described above) and BigchainDB, after trying for `BIGCHAINDB_DATABASE_MAXTRIES` times, gives up. The Kubernetes BigchainDB Deployment then restarts the BigchainDB pod.
2. BigchainDB crashes for some reason. We have seen this happen when updating BigchainDB from one version to the next. This usually means the older connections to the service gets disconnected; retrying the request one more time, forwards the connection to the new instance and succeed.

5.16.3 3. Service Unreachable

Communication between Kubernetes Services and Deployments fail in v1.6.6 and before due to a trivial key lookup error for non-existent services in the `kubelet`. This error can be reproduced by restarting any public facing (that is, services using the cloud load balancer) Kubernetes services, and watching the `kube-proxy` failure in its logs. The solution to this problem is to restart `kube-proxy` on the affected worker/agent node. Login to the worker node and run:

```
docker stop `docker ps | grep k8s_kube-proxy | cut -d" " -f1`

docker logs -f `docker ps | grep k8s_kube-proxy | cut -d" " -f1`
```

This issue is fixed in Kubernetes v1.7.

5.16.4 4. Single Disk Attached to Multiple Mountpoints in a Container

This is currently the issue faced in one of the clusters and being debugged by the support team at Microsoft.

The issue was first seen on August 29, 2017 on the Test Network and has been logged in the Azure/acs-engine repo on GitHub.

This is apparently fixed in Kubernetes v1.7.2 which include a new disk driver, but is yet to tested by us.

5.16.5 5. MongoDB Monitoring Agent throws a dial error while connecting to MongoDB

You might see something similar to this in the MongoDB Monitoring Agent logs:

```
Failure dialing host without auth. Err: `no reachable servers`
    at monitoring-agent/components/dialing.go:278
    at monitoring-agent/components/dialing.go:116
    at monitoring-agent/components/dialing.go:213
    at src/runtime/asm_amd64.s:2086
```

The first thing to check is if the networking is set up correctly. You can use the (maybe using the *toolbox* container).

If everything looks fine, it might be a problem with the `Preferred Hostnames` setting in MongoDB Cloud Manager. If you do need to change the regular expression, ensure that it is correct and saved properly (maybe try refreshing the MongoDB Cloud Manager web page to see if the setting sticks).

Once you update the regular expression, you will need to remove the deployment and add it again for the Monitoring Agent to discover and connect to the MongoDB instance correctly.

More information about this configuration is provided in *this document*.

5.16.6 6. Create a Persistent Volume from existing Azure disk storage Resource

When deleting a k8s cluster, all dynamically-created PVs are deleted, along with the underlying Azure storage disks (so those can't be used in a new cluster). resources are also deleted thus cannot be used in a new cluster. This workflow will preserve the Azure storage disks while deleting the k8s cluster and re-use the same disks on a new cluster for MongoDB persistent storage without losing any data.

The template to create two PVs for MongoDB Stateful Set (One for MongoDB data store and the other for MongoDB config store) is located at `mongodb/mongo-pv.yaml`.

You need to configure `diskName` and `diskURI` in `mongodb/mongo-pv.yaml` file. You can get these values by logging into your Azure portal and going to `Resource Groups` and click on your relevant resource group. From the list of resources click on the storage account resource and click the container (usually named as `vhds`) that contains storage disk blobs that are available for PVs. Click on the storage disk file that you wish to use for your PV and you will be able to see `NAME` and `URL` parameters which you can use for `diskName` and `diskURI` values in your template respectively and run the following command to create PVs:

```
$ kubectl --context <context-name> apply -f mongodb/mongo-pv.yaml
```

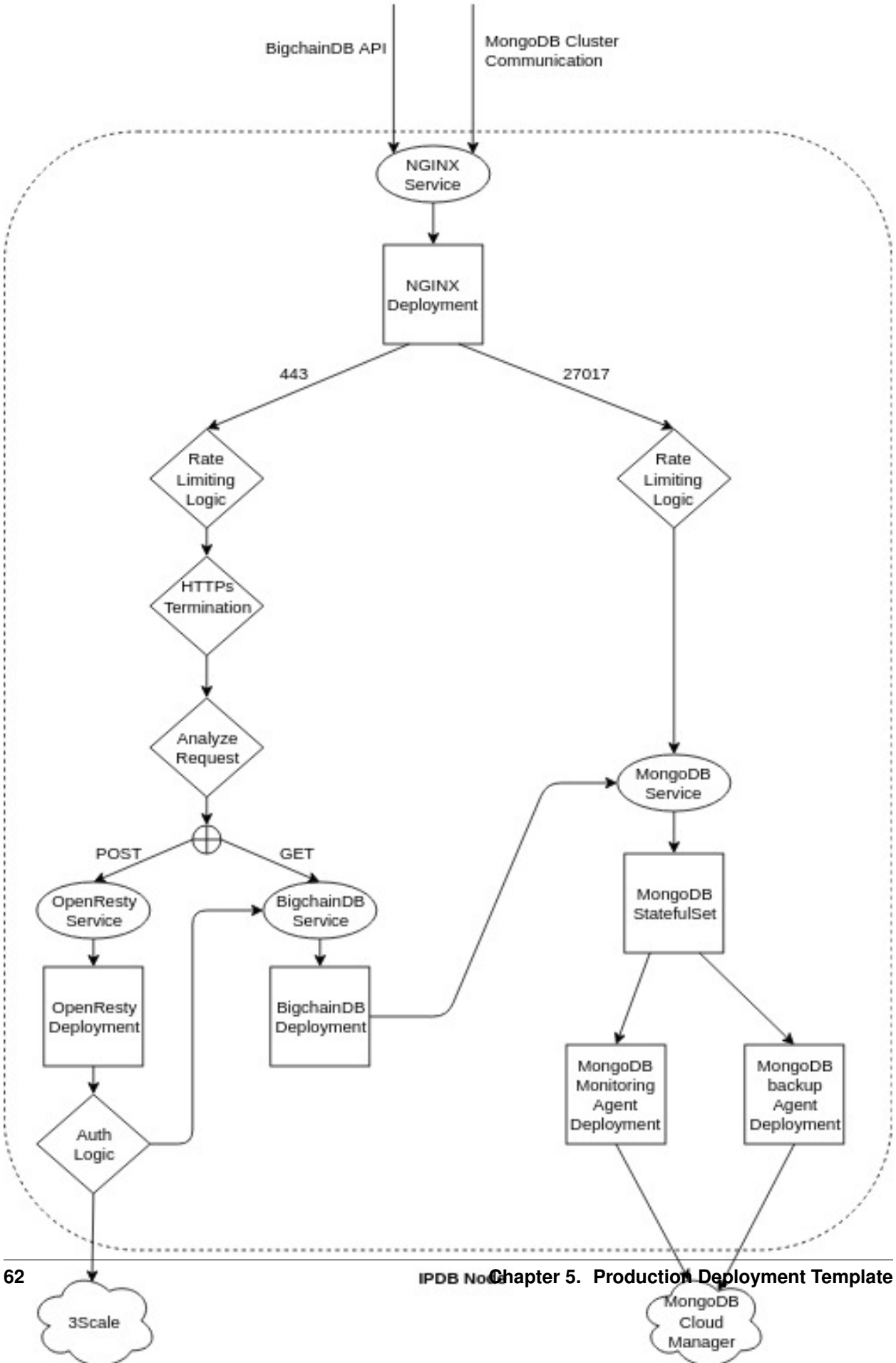
Note: Please make sure the storage disks you are using are not already being used by any other PVs. To check the existing PVs in your cluster, run the following command to get PVs and Storage disk file mapping.

```
$ kubectl --context <context-name> get pv --output yaml
```

5.17 Architecture of an IPDB Node

An IPDB Production deployment is hosted on a Kubernetes cluster and includes:

- NGINX, OpenResty, BigchainDB and MongoDB Kubernetes Services.
- NGINX, OpenResty, BigchainDB, Monitoring Agent and Backup Agent Kubernetes Deployments.
- MongoDB Kubernetes StatefulSet.
- Third party services like 3scale, MongoDB Cloud Manager and the Azure Operations Management Suite.


BigchainDB API
MongoDB Cluster Communication
NGINX Service
NGINX Deployment
443
27017
Rate Limiting Logic
Rate Limiting Logic
HTTPs Termination
Analyze Request
POST
GET
OpenResty Service
BigchainDB Service
MongoDB Service
MongoDB StatefulSet
OpenResty Deployment
BigchainDB Deployment
MongoDB Monitoring Agent Deployment
MongoDB backup Agent Deployment
Auth Logic
3Scale
MongoDB Cloud Manager

Note: The arrows in the diagram represent the client-server communication. For example, A–>B implies that A initiates the connection to B. It does not represent the flow of data; the communication channel is always fully duplex.

5.17.1 NGINX

We use an NGINX as HTTP proxy on port 443 (configurable) at the cloud entrypoint for:

1. Rate Limiting: We configure NGINX to allow only a certain number of requests (configurable) which prevents DoS attacks.
2. HTTPS Termination: The HTTPS connection does not carry through all the way to BigchainDB and terminates at NGINX for now.
3. Request Routing: For HTTPS connections on port 443 (or the configured BigchainDB public api port), the connection is proxied to:
   (a) OpenResty Service if it is a POST request.
   (b) BigchainDB Service if it is a GET request.

We use an NGINX TCP proxy on port 27017 (configurable) at the cloud entrypoint for:

1. Rate Limiting: We configure NGINX to allow only a certain number of requests (configurable) which prevents DoS attacks.
2. Request Routing: For connections on port 27017 (or the configured MongoDB public api port), the connection is proxied to the MongoDB Service.

5.17.2 OpenResty

We use OpenResty to perform authorization checks with 3scale using the `app_id` and `app_key` headers in the HTTP request.

OpenResty is NGINX plus a bunch of other components. We primarily depend on the LuaJIT compiler to execute the functions to authenticate the `app_id` and `app_key` with the 3scale backend.

5.17.3 MongoDB

We use MongoDB as the backend database for BigchainDB. In a multi-node deployment, MongoDB members communicate with each other via the public port exposed by the NGINX Service.

We achieve security by avoiding DoS attacks at the NGINX proxy layer and by ensuring that MongoDB has TLS enabled for all its connections.

CHAPTER 6

Develop & Test BigchainDB Server

This section outlines some ways that you could set up a minimal BigchainDB node for development and testing purposes. For additional guidance on how you could help develop BigchainDB, see the CONTRIBUTING.md file on GitHub.

6.1 Set Up BigchainDB Node on Local Dev Machine

The BigchainDB core dev team develops BigchainDB on recent Ubuntu, Fedora and CentOS distributions, so we recommend you use one of those. BigchainDB Server doesn't work on Windows or macOS (unless you use a VM or containers).

6.1.1 With MongoDB

First read the BigchainDB CONTRIBUTING.md file. It outlines the steps to set up a machine for developing and testing BigchainDB.

Create a default BigchainDB config file (in `$HOME/.bigchaindb`):

```
$ bigchaindb -y configure mongodb
```

Note: The BigchainDB CLI and the BigchainDB Configuration Settings are documented elsewhere. (Click the links.)

Start MongoDB **3.4+** using:

```
$ mongod --replSet=bigchain-rs
```

You can verify that MongoDB is running correctly by checking the output of the previous command for the line:

```
waiting for connections on port 27017
```

To run BigchainDB Server, do:

```
$ bigchaindb start
```

You can run all the unit tests to test your installation.

6.1.2 With RethinkDB

First read the BigchainDB CONTRIBUTING.md file. It outlines the steps to set up a machine for developing and testing BigchainDB.

Create a default BigchainDB config file (in `$HOME/.bigchaindb`):

```
$ bigchaindb -y configure rethinkdb
```

Note: The BigchainDB CLI and the BigchainDB Configuration Settings are documented elsewhere. (Click the links.)

Start RethinkDB using:

```
$ rethinkdb
```

You can verify that RethinkDB is running by opening the RethinkDB web interface in your web browser. It should be at http://localhost:8080/

To run BigchainDB Server, do:

```
$ bigchaindb start
```

You can run all the unit tests to test your installation.

6.2 Run BigchainDB with Docker

NOT for Production Use

For those who like using Docker and wish to experiment with BigchainDB in non-production environments, we currently maintain a Docker image and a `Dockerfile` that can be used to build an image for `bigchaindb`.

6.2.1 Prerequisite(s)

- Docker

6.2.2 Pull and Run the Image from Docker Hub

With Docker installed, you can proceed as follows.

In a terminal shell, pull the latest version of the BigchainDB Docker image using:

```
docker pull bigchaindb/bigchaindb
```

Configuration

A one-time configuration step is required to create the config file; we will use the `-y` option to accept all the default values. The configuration file will be stored in a file on your host machine at `~/bigchaindb_docker/.bigchaindb`:

```
docker run \
  --interactive \
  --rm \
  --tty \
  --volume $HOME/bigchaindb_docker:/data \
  --env BIGCHAINDB_DATABASE_HOST=172.17.0.1 \
  bigchaindb/bigchaindb \
  -y configure \
  [mongodb|rethinkdb]

Generating keypair
Configuration written to /data/.bigchaindb
Ready to go!
```

Let's analyze that command:

- `docker run` tells Docker to run some image
- `--interactive` keep STDIN open even if not attached
- `--rm` remove the container once we are done
- `--tty` allocate a pseudo-TTY
- `--volume "$HOME/bigchaindb_docker:/data"` map the host directory `$HOME/bigchaindb_docker` to the container directory `/data`; this allows us to have the data persisted on the host machine, you can read more in the official Docker documentation
- `--env BIGCHAINDB_DATABASE_HOST=172.17.0.1`, `172.17.0.1` is the default `docker0` bridge IP address, for fresh Docker installations. It is used for the communication between BigchainDB and database containers.
- `bigchaindb/bigchaindb` the image to use. All the options after the container name are passed on to the entrypoint inside the container.
- `-y configure` execute the `configure` sub-command (of the `bigchaindb` command) inside the container, with the `-y` option to automatically use all the default config values
- `mongodb` or `rethinkdb` specifies the database backend to use with bigchaindb

Run the backend database

From v0.9 onwards, you can run either RethinkDB or MongoDB.

You can also use docker host networking or bind to your primary (eth) interface, if needed.

For RethinkDB

```
docker run \
  --detach \
  --name=rethinkdb \
  --publish=28015:28015 \
```

```
  --publish=58080:8080 \
  --restart=always \
  --volume $HOME/bigchaindb_docker:/data \
  rethinkdb:2.3
```

You can also access the RethinkDB dashboard at http://172.17.0.1:58080/

For MongoDB

Note: MongoDB runs as user `mongodb` which had the UID `999` and GID `999` inside the container. For the volume to be mounted properly, as user `mongodb` in your host, you should have a `mongodb` user with UID and GID `999`. If you have another user on the host with UID `999`, the mapped files will be owned by this user in the host. If there is no owner with UID 999, you can create the corresponding user and group.

`useradd -r --uid 999 mongodb` OR `groupadd -r --gid 999 mongodb && useradd -r --uid 999 -g mongodb mongodb` should work.

```
docker run \
  --detach \
  --name=mongodb \
  --publish=27017:27017 \
  --restart=always \
  --volume=$HOME/mongodb_docker/db:/data/db \
  --volume=$HOME/mongodb_docker/configdb:/data/configdb \
  mongo:3.4.9 --replSet=bigchain-rs
```

Run BigchainDB

```
docker run \
  --detach \
  --name=bigchaindb \
  --publish=59984:9984 \
  --restart=always \
  --volume=$HOME/bigchaindb_docker:/data \
  bigchaindb/bigchaindb \
  start
```

The command is slightly different from the previous one, the differences are:

- `--detach` run the container in the background
- `--name bigchaindb` give a nice name to the container so it's easier to refer to it later
- `--publish "59984:9984"` map the host port `59984` to the container port `9984` (the BigchainDB API server)
- `start` start the BigchainDB service

Another way to publish the ports exposed by the container is to use the `-P` (or `--publish-all`) option. This will publish all exposed ports to random ports. You can always run `docker ps` to check the random mapping.

If that doesn't work, then replace `localhost` with the IP or hostname of the machine running the Docker engine. If you are running docker-machine (e.g. on Mac OS X) this will be the IP of the Docker machine (`docker-machine ip machine_name`).

6.2.3 Building Your Own Image

Assuming you have Docker installed, you would proceed as follows.

In a terminal shell:

```
git clone git@github.com:bigchaindb/bigchaindb.git
```

Build the Docker image:

```
docker build --tag local-bigchaindb .
```

Now you can use your own image to run BigchainDB containers.

6.3 Run BigchainDB with Vagrant

NOT for Production Use

You can use the following instructions to deploy a single or multi node BigchainDB setup for dev/test using Vagrant. Vagrant will set up the BigchainDB node(s) with all the dependencies along with MongoDB and BigchainDB Python driver. You can also tweak the following configurations for the BigchainDB node(s).

- Vagrant Box
  - Currently, we support the following boxes:
    - `ubuntu/xenial64 # >=16.04`
    - `centos/7 # >=7`
    - `fedora/24 # >=24`
  - **NOTE** : You can choose any other vagrant box of your choice but these are the minimum versioning requirements.
- Resources and specs for your box.
  - RAM
  - VCPUs
  - Network Type
    - Currently, only `private_network` is supported.
  - IP Address
- Deploy node with Docker
  - Deploy all the services in Docker containers or as processes.
- Number of BigchainDB nodes
  - If you want to deploy the services inside Docker containers, you can specify number of member(s) in the BigchainDB cluster.
- Upstart Script
- Vagrant Provider
  - Virtualbox
  - VMware

6.3.1 Minimum Requirements | Vagrant

Minimum resource requirements for a single node BigchainDB dev setup. **The more the better**:

- Memory >= 512MB
- VCPUs >= 1

6.3.2 Install dependencies | Vagrant

1. VirtualBox >= 5.0.0
2. Vagrant >= 1.16.0

6.3.3 Clone the BigchainDB repository | Vagrant

```
$ git clone https://github.com/bigchaindb/bigchaindb.git
```

6.3.4 Configuration | Vagrant

Navigate to `bigchaindb/pkg/configuration/vars/` inside the BigchainDB repository.

```
$ cd bigchaindb/pkg/configuration/vars/
```

Edit `bdb-config.yml` as per your requirements. Sample `bdb-config.yml`:

```
---
deploy_docker: false #[true, false]
docker_cluster_size: 1
upstart: "/bigchaindb/scripts/bootstrap.sh"
bdb_hosts:
  - name: "bdb-node-01"
    box:
      name: "ubuntu/xenial64"
    ram: "2048"
    vcpus: "2"
    network:
      ip: "10.20.30.40"
      type: "private_network"
```

Note: You can spawn multiple instances to orchestrate a multi-node BigchainDB cluster. Here is a sample `bdb-config.yml`:

```
---
deploy_docker: false #[true, false]
docker_cluster_size: 1
upstart: "/bigchaindb/scripts/bootstrap.sh"
bdb_hosts:
  - name: "bdb-node-01"
    box:
      name: "ubuntu/xenial64"
    ram: "2048"
    vcpus: "2"
    network:
      ip: "10.20.30.40"
```

```
      type: "private_network"
  - name: "bdb-node-02"
    box:
      name: "ubuntu/xenial64"
    ram: "2048"
    vcpus: "2"
    network:
      ip: "10.20.30.50"
      type: "private_network"
```

Note: You can also orchestrate a multi-node BigchainDB cluster on a single dev host using Docker containers. Here is a sample `bdb-config.yml`

```
---
deploy_docker: true #[true, false]
docker_cluster_size: 3
upstart: "/bigchaindb/scripts/bootstrap.sh"
bdb_hosts:
  - name: "bdb-node-01"
    box:
      name: "ubuntu/xenial64"
    ram: "8192"
    vcpus: "4"
    network:
      ip: "10.20.30.40"
      type: "private_network"
```

The above mentioned configuration will deploy a 3 node BigchainDB cluster with Docker containers on your specified host.

6.3.5 BigchainDB Setup | Vagrant

Note: There are some vagrant plugins required for the installation, user will be prompted to install them if they are not present. To install the required plugins, run the following command:

```
$ vagrant plugin install vagrant-cachier vagrant-vbguest vagrant-hosts
```

To bring up the BigchainDB node(s), run the following command:

```
$ vagrant up
```

After successful execution of Vagrant, you can log in to your fresh BigchainDB node.

```
$ vagrant ssh <instance-name>
```

6.3.6 Make your first transaction

Once you are inside the BigchainDB node, you can verify that BigchainDB docker(s)/process(es) is(are) running.

Verify BigchainDB process(es):

```
$ ps -ef | grep bigchaindb
```

OR

Verify BigchainDB Docker(s):

```
$ docker ps | grep bigchaindb
```

The BigchainDB Python Driver is pre-installed in the instance, so you can use it to make transactions and verify the functionality of your BigchainDB node. See the BigchainDB Python Driver documentation for details on how to use it.

Note 1: The `bdb_root_url` can be one of the following:

```
# BigchainDB is running as a process
bdb_root_url = http://<HOST-IP>:9984

OR

# BigchainDB is running inside a docker container
bdb_root_url = http://<HOST-IP>:<DOCKER-PUBLISHED-HOST-PORT>
```

Note 2: BigchainDB has other drivers as well.

6.4 Run BigchainDB with Ansible

NOT for Production Use

You can use the following instructions to deploy a single or multi node BigchainDB setup for dev/test using Ansible. Ansible will setup BigchainDB node(s) along with Docker, Docker Compose, MongoDB, BigchainDB Python driver.

Currently, this workflow is only supported for the following distributions:

- Ubuntu >= 16.04
- CentOS >= 7
- Fedora >= 24

6.4.1 Minimum Requirements | Ansible

Minimum resource requirements for a single node BigchainDB dev setup. **The more the better**:

- Memory >= 512MB
- VCPUs >= 1

6.4.2 Clone the BigchainDB repository | Ansible

```
$ git clone https://github.com/bigchaindb/bigchaindb.git
```

6.4.3 Install dependencies | Ansible

- Ansible

You can also install `ansible` and other dependencies, if any, using the `boostrap.sh` script inside the BigchainDB repository. Navigate to `bigchaindb/pkg/scripts` and run the `bootstrap.sh` script to install the dependecies for your OS. The script also checks if the OS you are running is compatible with the supported versions.

Note: `bootstrap.sh` only supports Ubuntu >= 16.04, CentOS >= 7 and Fedora >=24.

```
$ cd bigchaindb/pkg/scripts/
$ sudo ./bootstrap.sh
```

BigchainDB Setup Configuration(s) | Ansible

Local Setup | Ansible

You can run the Ansible playbook `bdb-deploy.yml` on your local dev machine and set up the BigchainDB node where BigchainDB can be run as a process or inside a Docker container(s) depending on your configuration.

Before, running the playbook locally, you need to update the `hosts` and `bdb-config.yml` configuration, which will notify Ansible that we need to run the play locally.

Update Hosts | Local

Navigate to `bigchaindb/pkg/configuration/hosts` inside the BigchainDB repository.

```
$ cd bigchaindb/pkg/configuration/hosts
```

Edit `all` configuration file:

```
# Delete any existing configuration in this file and insert
# Hostname of dev machine
<HOSTNAME> ansible_connection=local
```

Update Configuration | Local

Navigate to `bigchaindb/pkg/configuration/vars` inside the BigchainDB repository.

```
$ cd bigchaindb/pkg/configuration/vars/bdb-config.yml
```

Edit `bdb-config.yml` configuration file as per your requirements, sample configuration file(s):

```
---
deploy_docker: false #[true, false]
docker_cluster_size: 1 # Only needed if `deploy_docker` is true
bdb_hosts:
  - name: "<HOSTNAME>" # Hostname of dev machine
```

Note: You can also orchestrate a multi-node BigchainDB cluster on a local dev host using Docker containers. Here is a sample `bdb-config.yml`

```
---
deploy_docker: true #[true, false]
docker_cluster_size: 3
bdb_hosts:
  - name: "<LOCAL_DEV_HOST_HOSTNAME>"
```

BigchainDB Setup | Ansible

Now, You can safely run the `bdb-deploy.yml` playbook and everything will be taken care of by `Ansible`. To run the playbook please navigate to the `bigchaindb/pkg/configuration` directory inside the BigchainDB repository and run the `bdb-deploy.yml` playbook.

```
$ cd bigchaindb/pkg/configuration/

$ sudo ansible-playbook bdb-deploy.yml -i hosts/all
```

After successful execution of the playbook, you can verify that BigchainDB docker(s)/process(es) is(are) running.

Verify BigchainDB process(es):

```
$ ps -ef | grep bigchaindb
```

OR

Verify BigchainDB Docker(s):

```
$ docker ps | grep bigchaindb
```

The playbook also installs the BigchainDB Python Driver, so you can use it to make transactions and verify the functionality of your BigchainDB node. See the BigchainDB Python Driver documentation for details on how to use it.

Note: The `bdb_root_url` can be be one of the following:

```
# BigchainDB is running as a process
bdb_root_url = http://<HOST-IP>:9984

OR

# BigchainDB is running inside a docker container
bdb_root_url = http://<HOST-IP>:<DOCKER-PUBLISHED-PORT>
```

Note: BigchainDB has other drivers as well.

Experimental: Running Ansible a Remote Dev/Host

Remote Setup | Ansible

You can also run the Ansible playbook `bdb-deploy.yml` on remote machine(s) and set up the BigchainDB node where BigchainDB can run as a process or inside a Docker container(s) depending on your configuration.

Before, running the playbook on a remote host, you need to update the `hosts` and `bdb-config.yml` configuration, which will notify Ansible that we need to run the play on a remote host.

Update Hosts | Remote

Navigate to `bigchaindb/pkg/configuration/hosts` inside the BigchainDB repository.

```
$ cd bigchaindb/pkg/configuration/hosts
```

Edit `all` configuration file:

```
# Delete any existing configuration in this file and insert
<Remote_Host_IP/Hostname> ansible_ssh_user=<USERNAME> ansible_sudo_pass=<ROOT_
↪PASSWORD>
```

Note: You can add multiple hosts to the `all` configuration file. Root password is needed because ansible will run some tasks that require root permissions.

Note: You can also use other methods to get inside the remote machines instead of password based SSH. For other methods please consult Ansible Documentation.

Update Configuration | Remote

Navigate to `bigchaindb/pkg/configuration/vars` inside the BigchainDB repository.

```
$ cd bigchaindb/pkg/configuration/vars/bdb-config.yml
```

Edit `bdb-config.yml` configuration file as per your requirements, sample configuration file(s):

```
---
deploy_docker: false #[true, false]
docker_cluster_size: 1 # Only needed if `deploy_docker` is true
bdb_hosts:
  - name: "<REMOTE_MACHINE_HOSTNAME>"
```

After, the configuration of remote hosts, *run the Ansible playbook and verify your deployment*.

6.5 Running All Tests

All documentation about writing and running tests (unit and integration tests) was moved to the file `bigchaindb/tests/README.md`.

CHAPTER 7

Settings & CLI

7.1 Configuration Settings

The value of each BigchainDB Server configuration setting is determined according to the following rules:

- If it's set by an environment variable, then use that value
- Otherwise, if it's set in a local config file, then use that value
- Otherwise, use the default value

For convenience, here's a list of all the relevant environment variables (documented below):

```
BIGCHAINDB_KEYPAIR_PUBLIC     BIGCHAINDB_KEYPAIR_PRIVATE     BIGCHAINDB_KEYRING
BIGCHAINDB_DATABASE_BACKEND  BIGCHAINDB_DATABASE_HOST  BIGCHAINDB_DATABASE_PORT
BIGCHAINDB_DATABASE_NAME BIGCHAINDB_DATABASE_REPLICASET BIGCHAINDB_DATABASE_CONNECTION_TIMEO
BIGCHAINDB_DATABASE_MAX_TRIES BIGCHAINDB_SERVER_BIND BIGCHAINDB_SERVER_LOGLEVEL
BIGCHAINDB_SERVER_WORKERS  BIGCHAINDB_WSSERVER_SCHEME  BIGCHAINDB_WSSERVER_HOST
BIGCHAINDB_WSSERVER_PORT                  BIGCHAINDB_WSSERVER_ADVERTISED_SCHEME
BIGCHAINDB_WSSERVER_ADVERTISED_HOST         BIGCHAINDB_WSSERVER_ADVERTISED_PORT
BIGCHAINDB_CONFIG_PATH     BIGCHAINDB_BACKLOG_REASSIGN_DELAY     BIGCHAINDB_LOG
BIGCHAINDB_LOG_FILE   BIGCHAINDB_LOG_ERROR_FILE   BIGCHAINDB_LOG_LEVEL_CONSOLE
BIGCHAINDB_LOG_LEVEL_LOGFILE                      BIGCHAINDB_LOG_DATEFMT_CONSOLE
BIGCHAINDB_LOG_DATEFMT_LOGFILE                        BIGCHAINDB_LOG_FMT_CONSOLE
BIGCHAINDB_LOG_FMT_LOGFILE  BIGCHAINDB_LOG_GRANULAR_LEVELS  BIGCHAINDB_LOG_PORT
BIGCHAINDB_DATABASE_SSL BIGCHAINDB_DATABASE_LOGIN BIGCHAINDB_DATABASE_PASSWORD
BIGCHAINDB_DATABASE_CA_CERT BIGCHAINDB_DATABASE_CERTFILE BIGCHAINDB_DATABASE_KEYFILE
BIGCHAINDB_DATABASE_KEYFILE_PASSPHRASE              BIGCHAINDB_DATABASE_CRLFILE
BIGCHAINDB_GRAPHITE_HOST
```

The local config file is `$HOME/.bigchaindb` by default (a file which might not even exist), but you can tell BigchainDB to use a different file by using the `-c` command-line option, e.g. `bigchaindb -c path/to/config_file.json start` or using the `BIGCHAINDB_CONFIG_PATH` environment variable, e.g. `BIGHAINDB_CONFIG_PATH=.my_bigchaindb_config bigchaindb start`. Note that the `-c` command line option will always take precedence if both the `BIGCHAINDB_CONFIG_PATH` and the `-c` command line

option are used.

You can read the current default values in the file bigchaindb/__init__.py. (The link is to the latest version.)

Running `bigchaindb -y configure mongodb` will generate a local config file in `$HOME/.bigchaindb` with all the default values (for using MongoDB as the database backend), with two exceptions: it will generate a valid private/public keypair, rather than using the default keypair (`None` and `None`).

7.1.1 keypair.public & keypair.private

The cryptographic keypair used by the node. The public key is how the node idenifies itself to the world. The private key is used to generate cryptographic signatures. Anyone with the public key can verify that the signature was generated by whoever had the corresponding private key.

Example using environment variables

```
export BIGCHAINDB_KEYPAIR_PUBLIC=8wHUvvraRo5yEoJAt66UTZaFq9YZ9tFFwcauKPDtjkGw
export BIGCHAINDB_KEYPAIR_PRIVATE=5C5Cknco7YxBRP9AgB1cbUVTL4FAcooxErLygw1DeG2D
```

Example config file snippet

```
"keypair": {
  "public": "8wHUvvraRo5yEoJAt66UTZaFq9YZ9tFFwcauKPDtjkGw",
  "private": "5C5Cknco7YxBRP9AgB1cbUVTL4FAcooxErLygw1DeG2D"
}
```

Internally (i.e. in the Python code), both keys have a default value of `None`, but that's not a valid key. Therefore you can't rely on the defaults for the keypair. If you want to run BigchainDB, you must provide a valid keypair, either in the environment variables or in the local config file. You can generate a local config file with a valid keypair (and default everything else) using `bigchaindb -y configure mongodb`.

7.1.2 keyring

A list of the public keys of all the nodes in the cluster, excluding the public key of this node.

Example using an environment variable

```
export BIGCHAINDB_
↪KEYRING=BnCsre9MPBeQK8QZBFznU2dJJ2GwtvnSMdemCmod2XPB:4cYQHoQrvPiut3Sjs8fVR1BMZZpJjMTC4bsMTt9V71aQ
```

Note how the keys in the list are separated by colons.

Example config file snippet

```
"keyring": ["BnCsre9MPBeQK8QZBFznU2dJJ2GwtvnSMdemCmod2XPB",
            "4cYQHoQrvPiut3Sjs8fVR1BMZZpJjMTC4bsMTt9V71aQ"]
```

Default value (from a config file)

```
"keyring": []
```

7.1.3 database.*

The settings with names of the form `database.*` are for the database backend (currently either MongoDB or RethinkDB). They are:

- `database.backend` is either `mongodb` or `rethinkdb`.
- `database.host` is the hostname (FQDN) of the backend database.
- `database.port` is self-explanatory.
- `database.name` is a user-chosen name for the database inside MongoDB or RethinkDB, e.g. `bigchain`.
- `database.replicaset` is only relevant if using MongoDB; it's the name of the MongoDB replica set, e.g. `bigchain-rs`.
- `database.connection_timeout` is the maximum number of milliseconds that BigchainDB will wait before giving up on one attempt to connect to the database backend.
- `database.max_tries` is the maximum number of times that BigchainDB will try to establish a connection with the database backend. If 0, then it will try forever.
- `database.ssl` is a flag that determines if BigchainDB connects to the backend database over TLS/SSL or not. This can be set to either `true` or `false` (the default). Note: This parameter is only supported for the MongoDB backend currently.
- `database.login` and `database.password` are the login and password used to authenticate to the database before performing any operations, specified in plaintext. The default values for both are currently `null`, which means that BigchainDB will not authenticate with the backend database. Note: These parameters are only supported for the MongoDB backend currently.
- `database.ca_cert`, `database.certfile`, `database.keyfile` and `database.crlfile` are the paths to the CA, signed certificate, private key and certificate revocation list files respectively. Note: These parameters are only supported for the MongoDB backend currently.
- `database.keyfile_passphrase` is the private key decryption passphrase, specified in plaintext. Note: This parameter is only supported for the MongoDB backend currently.

Example using environment variables

```
export BIGCHAINDB_DATABASE_BACKEND=mongodb
export BIGCHAINDB_DATABASE_HOST=localhost
export BIGCHAINDB_DATABASE_PORT=27017
export BIGCHAINDB_DATABASE_NAME=bigchain
export BIGCHAINDB_DATABASE_REPLICASET=bigchain-rs
export BIGCHAINDB_DATABASE_CONNECTION_TIMEOUT=5000
export BIGCHAINDB_DATABASE_MAX_TRIES=3
```

Default values

If (no environment variables were set and there's no local config file), or you used `bigchaindb -y configure rethinkdb` to create a default local config file for a RethinkDB backend, then the defaults will be:

```
"database": {
    "backend": "rethinkdb",
    "host": "localhost",
    "port": 28015,
    "name": "bigchain",
    "connection_timeout": 5000,
    "max_tries": 3
}
```

If you used `bigchaindb -y configure mongodb` to create a default local config file for a MongoDB backend, then the defaults will be:

```
"database": {
    "backend": "mongodb",
    "host": "localhost",
    "port": 27017,
    "name": "bigchain",
    "replicaset": "bigchain-rs",
    "connection_timeout": 5000,
    "max_tries": 3,
    "login": null,
    "password": null
    "ssl": false,
    "ca_cert": null,
    "crlfile": null,
    "certfile": null,
    "keyfile": null,
    "keyfile_passphrase": null,
}
```

7.1.4 server.bind, server.loglevel & server.workers

These settings are for the Gunicorn HTTP server, which is used to serve the HTTP client-server API.

`server.bind` is where to bind the Gunicorn HTTP server socket. It's a string. It can be any valid value for Gunicorn's bind setting. If you want to allow IPv4 connections from anyone, on port 9984, use `0.0.0.0:9984`. In a production setting, we recommend you use Gunicorn behind a reverse proxy server. If Gunicorn and the reverse proxy are running on the same machine, then use `localhost:PORT` where PORT is *not* 9984 (because the reverse proxy needs to listen on port 9984). Maybe use PORT=9983 in that case because we know 9983 isn't used. If Gunicorn and the reverse proxy are running on different machines, then use `A.B.C.D:9984` where A.B.C.D is the IP address of the reverse proxy. There's more information about deploying behind a reverse proxy in the Gunicorn documentation. (They call it a proxy.)

`server.loglevel` sets the log level of Gunicorn's Error log outputs. See Gunicorn's documentation for more information.

`server.workers` is the number of worker processes for handling requests. If `None` (the default), the value will be (2 × cpu_count + 1). Each worker process has a single thread. The HTTP server will be able to handle `server.workers` requests simultaneously.

Example using environment variables

```
export BIGCHAINDB_SERVER_BIND=0.0.0.0:9984
export BIGCHAINDB_SERVER_LOGLEVEL=debug
export BIGCHAINDB_SERVER_WORKERS=5
```

Example config file snippet

```
"server": {
    "bind": "0.0.0.0:9984",
    "loglevel": "debug",
    "workers": 5,
}
```

Default values (from a config file)

```
"server": {
    "bind": "localhost:9984",
    "loglevel": "info",
```

```
    "workers": null,
}
```

7.1.5 wsserver.scheme, wsserver.host and wsserver.port

These settings are for the aiohttp server, which is used to serve the WebSocket Event Stream API. `wsserver.scheme` should be either `"ws"` or `"wss"` (but setting it to `"wss"` does *not* enable SSL/TLS). `wsserver.host` is where to bind the aiohttp server socket and `wsserver.port` is the corresponding port. If you want to allow connections from anyone, on port 9985, set `wsserver.host` to 0.0.0.0 and `wsserver.port` to 9985.

Example using environment variables

```
export BIGCHAINDB_WSSERVER_SCHEME=ws
export BIGCHAINDB_WSSERVER_HOST=0.0.0.0
export BIGCHAINDB_WSSERVER_PORT=9985
```

Example config file snippet

```
"wsserver": {
    "scheme": "wss",
    "host": "0.0.0.0",
    "port": 65000
}
```

Default values (from a config file)

```
"wsserver": {
    "scheme": "ws",
    "host": "localhost",
    "port": 9985
}
```

7.1.6 wsserver.advertised_scheme, wsserver.advertised_host and wsserver.advertised_port

These settings are for the advertising the Websocket URL to external clients in the root API endpoint. These configurations might be useful if your deployment is hosted behind a firewall, NAT, etc. where the exposed public IP or domain is different from where BigchainDB is running.

Example using environment variables

```
export BIGCHAINDB_WSSERVER_ADVERTISED_SCHEME=wss
export BIGCHAINDB_WSSERVER_ADVERTISED_HOST=mybigchaindb.com
export BIGCHAINDB_WSSERVER_ADVERTISED_PORT=443
```

Example config file snippet

```
"wsserver": {
    "advertised_scheme": "wss",
    "advertised_host": "mybigchaindb.com",
    "advertised_port": 443
}
```

Default values (from a config file)

```
"wsserver": {
    "advertised_scheme": "ws",
    "advertised_host": "localhost",
    "advertised_port": 9985
}
```

7.1.7 backlog_reassign_delay

Specifies how long, in seconds, transactions can remain in the backlog before being reassigned. Long-waiting transactions must be reassigned because the assigned node may no longer be responsive. The default duration is 120 seconds.

Example using environment variables

```
export BIGCHAINDB_BACKLOG_REASSIGN_DELAY=30
```

Default value (from a config file)

```
"backlog_reassign_delay": 120
```

7.1.8 log

The `log` key is expected to point to a mapping (set of key/value pairs) holding the logging configuration.

Example:

```
{
    "log": {
        "file": "/var/log/bigchaindb.log",
        "error_file": "/var/log/bigchaindb-errors.log",
        "level_console": "info",
        "level_logfile": "info",
        "datefmt_console": "%Y-%m-%d %H:%M:%S",
        "datefmt_logfile": "%Y-%m-%d %H:%M:%S",
        "fmt_console": "%(asctime)s [%(levelname)s] (%(name)s) %(message)s",
        "fmt_logfile": "%(asctime)s [%(levelname)s] (%(name)s) %(message)s",
        "granular_levels": {
            "bichaindb.backend": "info",
            "bichaindb.core": "info"
        },
        "port": 7070
}
```

Defaults to:

```
{
    "log": {
        "file": "~/bigchaindb.log",
        "error_file": "~/bigchaindb-errors.log",
        "level_console": "info",
        "level_logfile": "info",
        "datefmt_console": "%Y-%m-%d %H:%M:%S",
        "datefmt_logfile": "%Y-%m-%d %H:%M:%S",
        "fmt_logfile": "[%(asctime)s] [%(levelname)s] (%(name)s) %(message)s (
↪%(processName)-10s - pid: %(process)d)",
```

```
        "fmt_console": "[%(asctime)s] [%(levelname)s] (%(name)s) %(message)s (
↪%(processName)-10s - pid: %(process)d)",
        "granular_levels": {},
        "port": 9020
}
```

The next subsections explain each field of the `log` configuration.

log.file & log.error_file

The full paths to the files where logs and error logs should be written to.

Example:

```
{
    "log": {
        "file": "/var/log/bigchaindb/bigchaindb.log"
        "error_file": "/var/log/bigchaindb/bigchaindb-errors.log"
    }
}
```

Defaults to:

```
* `"~/bigchaindb.log"`
* `"~/bigchaindb-errors.log"`
```

Please note that the user running `bigchaindb` must have write access to the locations.

Log rotation

Log files have a size limit of 200 MB and will be rotated up to five times.

For example if we consider the log file setting:

```
{
    "log": {
        "file": "~/bigchain.log"
    }
}
```

logs would always be written to `bigchain.log`. Each time the file `bigchain.log` reaches 200 MB it would be closed and renamed `bigchain.log.1`. If `bigchain.log.1` and `bigchain.log.2` already exist they would be renamed `bigchain.log.2` and `bigchain.log.3`. This pattern would be applied up to `bigchain.log.5` after which `bigchain.log.5` would be overwritten by `bigchain.log.4`, thus ending the rotation cycle of whatever logs were in `bigchain.log.5`.

log.level_console

The log level used to log to the console. Possible allowed values are the ones defined by Python, but case insensitive for convenience's sake:

```
"critical", "error", "warning", "info", "debug", "notset"
```

Example:

```
{
    "log": {
        "level_console": "info"
    }
}
```

Defaults to: `"info"`.

log.level_logfile

The log level used to log to the log file. Possible allowed values are the ones defined by Python, but case insensitive for convenience's sake:

```
"critical", "error", "warning", "info", "debug", "notset"
```

Example:

```
{
    "log": {
        "level_file": "info"
    }
}
```

Defaults to: `"info"`.

log.datefmt_console

The format string for the date/time portion of a message, when logged to the console.

Example:

```
{
    "log": {
        "datefmt_console": "%x %X %Z"
    }
}
```

Defaults to: `"%Y-%m-%d %H:%M:%S"`.

For more information on how to construct the format string please consult the table under Python's documentation of `time.strftime(format[, t])`

log.datefmt_logfile

The format string for the date/time portion of a message, when logged to a log file.

Example:

```
{
    "log": {
        "datefmt_logfile": "%c %z"
    }
}
```

Defaults to: `"%Y-%m-%d %H:%M:%S"`.

For more information on how to construct the format string please consult the table under Python's documentation of `time.strftime(format[, t])`

log.fmt_console

A string used to format the log messages when logged to the console.

Example:

```
{
    "log": {
        "fmt_console": "%(asctime)s [%(levelname)s] %(message)s %(process)d"
    }
}
```

Defaults to: `"[%(asctime)s] [%(levelname)s] (%(name)s) %(message)s (%(processName)-10s - pid: %(process)d)"`

For more information on possible formatting options please consult Python's documentation on LogRecord attributes

log.fmt_logfile

A string used to format the log messages when logged to a log file.

Example:

```
{
    "log": {
        "fmt_logfile": "%(asctime)s [%(levelname)s] %(message)s %(process)d"
    }
}
```

Defaults to: `"[%(asctime)s] [%(levelname)s] (%(name)s) %(message)s (%(processName)-10s - pid: %(process)d)"`

For more information on possible formatting options please consult Python's documentation on LogRecord attributes

log.granular_levels

Log levels for BigchainDB's modules. This can be useful to control the log level of specific parts of the application. As an example, if you wanted the logging of the `core.py` module to be more verbose, you would set the configuration shown in the example below.

Example:

```
{
    "log": {
        "granular_levels": {
            "bichaindb.core": "debug"
        }
}
```

Defaults to: `{}`

log.port

The port number at which the logging server should listen.

Example:

```
{
    "log": {
        "port": 7070
        }
}
```

Defaults to: `9020`

7.1.9 graphite.host

The host name or IP address of a server listening for statsd events on UDP port 8125. This defaults to `localhost`, and if no statsd collector is running, the events are simply dropped by the operating system.

Example using environment variables

```
export BIGCHAINDB_GRAPHITE_HOST=10.0.0.5
```

Example config file snippet

```
"graphite": {
    "host": "10.0.0.5"
}
```

Default values (from a config file)

```
"graphite": {
    "host": "localhost"
}
```

7.2 Command Line Interface (CLI)

The command-line command to interact with BigchainDB Server is `bigchaindb`.

7.2.1 bigchaindb –help

Show help for the `bigchaindb` command. `bigchaindb -h` does the same thing.

7.2.2 bigchaindb –version

Show the version number. `bigchaindb -v` does the same thing.

7.2.3 bigchaindb configure

Generate a local configuration file (which can be used to set some or all BigchainDB node configuration settings). It will auto-generate a public-private keypair and then ask you for the values of other configuration settings. If you press Enter for a value, it will use the default value.

Since BigchainDB supports multiple databases you need to always specify the database backend that you want to use. At this point only two database backends are supported: `rethinkdb` and `mongodb`.

If you use the `-c` command-line option, it will generate the file at the specified path:

```
bigchaindb -c path/to/new_config.json configure rethinkdb
```

If you don't use the `-c` command-line option, the file will be written to `$HOME/.bigchaindb` (the default location where BigchainDB looks for a config file, if one isn't specified).

If you use the `-y` command-line option, then there won't be any interactive prompts: it will just generate a keypair and use the default values for all the other configuration settings.

```
bigchaindb -y configure rethinkdb
```

7.2.4 bigchaindb show-config

Show the values of the BigchainDB node configuration settings.

7.2.5 bigchaindb export-my-pubkey

Write the node's public key (i.e. one of its configuration values) to standard output (stdout).

7.2.6 bigchaindb init

Create a backend database (RethinkDB or MongoDB), all database tables/collections, various backend database indexes, and the genesis block.

7.2.7 bigchaindb drop

Drop (erase) the backend database (a RethinkDB or MongoDB database). You will be prompted to make sure. If you want to force-drop the database (i.e. skipping the yes/no prompt), then use `bigchaindb -y drop`

7.2.8 bigchaindb start

Start BigchainDB. It always begins by trying a `bigchaindb init` first. See the note in the documentation for `bigchaindb init`. The database initialization step is optional and can be skipped by passing the `--no-init` flag i.e. `bigchaindb start --no-init`. You can also use the `--dev-start-rethinkdb` command line option to automatically start rethinkdb with bigchaindb if rethinkdb is not already running, e.g. `bigchaindb --dev-start-rethinkdb start`. Note that this will also shutdown rethinkdb when the bigchaindb process stops. The option `--dev-allow-temp-keypair` will generate a keypair on the fly if no keypair is found, this is useful when you want to run a temporary instance of BigchainDB in a Docker container, for example.

Options

The log level for the console can be set via the option `--log-level` or its abbreviation `-l`. Example:

```
$ bigchaindb --log-level INFO start
```

The allowed levels are `DEBUG`, `INFO` , `WARNING`, `ERROR`, and `CRITICAL`. For an explanation regarding these levels please consult the Logging Levels section of Python's documentation.

For a more fine-grained control over the logging configuration you can use the configuration file as documented under Configuration Settings.

7.2.9 bigchaindb set-shards

This command is specific to RethinkDB so it will only run if BigchainDB is configured with `rethinkdb` as the backend.

If RethinkDB is the backend database, then:

```
$ bigchaindb set-shards 4
```

will set the number of shards (in all RethinkDB tables) to 4.

7.2.10 bigchaindb set-replicas

This command is specific to RethinkDB so it will only run if BigchainDB is configured with `rethinkdb` as the backend.

If RethinkDB is the backend database, then:

```
$ bigchaindb set-replicas 3
```

will set the number of replicas (of each shard) to 3 (i.e. it will set the replication factor to 3).

7.2.11 bigchaindb add-replicas

This command is specific to MongoDB so it will only run if BigchainDB is configured with `mongodb` as the backend.

This command is used to add nodes to a BigchainDB cluster. It accepts a list of space separated hosts in the form *hostname:port*:

```
$ bigchaindb add-replicas server1.com:27017 server2.com:27017 server3.com:27017
```

7.2.12 bigchaindb remove-replicas

This command is specific to MongoDB so it will only run if BigchainDB is configured with `mongodb` as the backend.

This command is used to remove nodes from a BigchainDB cluster. It accepts a list of space separated hosts in the form *hostname:port*:

```
$ bigchaindb remove-replicas server1.com:27017 server2.com:27017 server3.com:27017
```

CHAPTER 8

The HTTP Client-Server API

This page assumes you already know an API Root URL for a BigchainDB node or reverse proxy. It should be something like `https://example.com:9984` or `https://12.34.56.78:9984`.

If you set up a BigchainDB node or reverse proxy yourself, and you're not sure what the API Root URL is, then see the last section of this page for help.

8.1 BigchainDB Root URL

If you send an HTTP GET request to the BigchainDB Root URL e.g. `http://localhost:9984` or `https://example.com:9984` (with no `/api/v1/` on the end), then you should get an HTTP response with something like the following in the body:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "api": {
    "v1": {
      "assets": "/api/v1/assets/",
      "docs": "https://docs.bigchaindb.com/projects/server/en/v1.3.0/http-client-
↪server-api.html",
      "outputs": "/api/v1/outputs/",
      "statuses": "/api/v1/statuses/",
      "streams": "ws://localhost:9985/api/v1/streams/valid_transactions",
      "transactions": "/api/v1/transactions/"
    }
  },
  "docs": "https://docs.bigchaindb.com/projects/server/en/v1.3.0/",
  "keyring": [
    "6qHyZew94NMmUTYyHnkZsB8cxJYuRNEiEpXHe1ih9QX3",
    "AdDuyrTyjrDt935YnFu4VBCVDhHtY2Y6rcy7x2TFeiRi"
  ],
  "public_key": "NC8c8rYcAhyKVpx1PCV65CBmyq4YUbLysy3Rqrg8L8mz",
```

```
  "software": "BigchainDB",
  "version": "1.3.0"
}
```

8.2 API Root Endpoint

If you send an HTTP GET request to the API Root Endpoint e.g. `http://localhost:9984/api/v1/` or `https://example.com:9984/api/v1/`, then you should get an HTTP response that allows you to discover the BigchainDB API endpoints:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "assets": "/assets/",
  "docs": "https://docs.bigchaindb.com/projects/server/en/v1.3.0/http-client-server-
↪api.html",
  "outputs": "/outputs/",
  "statuses": "/statuses/",
  "streams": "ws://localhost:9985/api/v1/streams/valid_transactions",
  "transactions": "/transactions/"
}
```

8.3 Transactions

GET /api/v1/transactions/{transaction_id}

Get the transaction with the ID `transaction_id`.

This endpoint returns a transaction if it was included in a `VALID` block. All instances of a transaction in invalid/undecided blocks or the backlog are ignored and treated as if they don't exist. If a request is made for a transaction and instances of that transaction are found only in invalid/undecided blocks or the backlog, then the response will be `404 Not Found`.

Parameters

- **transaction_id** (*hex string*) – transaction ID

Example request:

```
GET /api/v1/transactions/
↪8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "asset": {
    "data": {
      "msg": "Hello BigchainDB!"
    }
  },
```

```
  "id": "8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102",
  "inputs": [
    {
      "fulfillment": "pGSAIDE5i63cn4X8T8N1sZ2mGkJD5lNRnBM4PZgI_zvzbr-
↪cgUCGvCc2HO2uB4IKix6INRzGIM10r7VsKFMPM9cT7uVJ1xFLOJ9bn6UioepBMLIrrwTlk2CkTolIPonf7BnzriQL
↪",
      "fulfills": null,
      "owners_before": [
        "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
      ]
    }
  ],
  "metadata": {
    "sequence": 0
  },
  "operation": "CREATE",
  "outputs": [
    {
      "amount": "1",
      "condition": {
        "details": {
          "public_key": "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD",
          "type": "ed25519-sha-256"
        },
        "uri": "ni:///sha-256;PNYwdxaRaNw60N6LDFzOWO97b8tJeragczakL8PrAPc?
↪fpt=ed25519-sha-256&cost=131072"
      },
      "public_keys": [
        "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
      ]
    }
  ],
  "version": "1.0"
}
```


Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – A transaction with that ID was found.
- 404 Not Found – A transaction with that ID was not found.

`GET /api/v1/transactions`

The unfiltered `/api/v1/transactions` endpoint without any query parameters returns a status code *400*. For valid filters, see the sections below.

There are however filtered requests that might come of use, given the endpoint is queried correctly. Some of them include retrieving a list of transactions that include:

- *Transactions related to a specific asset*

In this section, we've listed those particular requests, as they will likely to be very handy when implementing your application on top of BigchainDB.

Note: Looking up transactions with a specific `metadata` field is currently not supported, however, providing

a way to query based on `metadata` data is on our roadmap.

A generalization of those parameters follows:

Query Parameters

- **asset_id** (*string*) – The ID of the asset.
- **operation** (*string*) – (Optional) One of the two supported operations of a transaction: `CREATE`, `TRANSFER`.

GET /api/v1/transactions?asset_id={asset_id}&operation={CREATE|TRANSFER}

Get a list of transactions that use an asset with the ID `asset_id`. Every `TRANSFER` transaction that originates from a `CREATE` transaction with `asset_id` will be included. This allows users to query the entire history or provenance of an asset.

This endpoint returns transactions only if they are decided `VALID` by the server.

Query Parameters

- **operation** (*string*) – (Optional) One of the two supported operations of a transaction: `CREATE`, `TRANSFER`.
- **asset_id** (*string*) – asset ID.

Example request:

```
GET /api/v1/transactions?operation=TRANSFER&asset_
↪id=8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

[{
  "asset": {
    "id": "8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102"
  },
  "id": "7d3ed7e5bcad27b878a4e3f25363c8b03f49fa5007f6e6032d9ec38e36bc2e83",
  "inputs": [
    {
      "fulfillment": "pGSAIDE5i63cn4X8T8N1sZ2mGkJD5lNRnBM4PZgI_zvzbr-
↪cgUA11pDN83PjcBhuH-
↪ICqy6cbyxeXrHQBgHXhbulDInXoMPsVeOJp65Wsxr0WO6kmJvwgA7Je1UgzNJZ6pWb3kcL",
      "fulfills": {
        "output_index": 0,
        "transaction_id":
↪"8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102"
      },
      "owners_before": [
        "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
      ]
    }
  ],
  "metadata": {
    "sequence": 1
  },
  "operation": "TRANSFER",
  "outputs": [
```

```
    {
      "amount": "1",
      "condition": {
        "details": {
          "public_key": "3yfQPHeWAa1MxTX9Zf9176QqcpcnWcanVZZbaHb8B3h9",
          "type": "ed25519-sha-256"
        },
        "uri": "ni:///sha-256;lu6ov4AKkee6KWGnyjOVLBeyuP0bz4-O6_dPi15eYUc?
↪fpt=ed25519-sha-256&cost=131072"
      },
      "public_keys": [
        "3yfQPHeWAa1MxTX9Zf9176QqcpcnWcanVZZbaHb8B3h9"
      ]
    }
  ],
  "version": "1.0"
},
{
  "asset": {
    "id": "8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102"
  },
  "id": "d07285a60352838ff263a46ba8cca64e18d36888aee0ba76d5d601137b492fc6",
  "inputs": [
    {
      "fulfillment": "pGSAICw7Ul-c2lG6NFbHp3FbKRC7fivQcNGO7GS4wV3A-
↪1QggUBRFFWoFwJhWGhbt02I3NPIBT84qzNB1-
↪dTyuj1zvUfVmY7fn1GAqI6A6pPRch36hYF4Gup2R0DFdAitEHxhB4K",
      "fulfills": {
        "output_index": 0,
        "transaction_id":
↪"7d3ed7e5bcad27b878a4e3f25363c8b03f49fa5007f6e6032d9ec38e36bc2e83"
      },
      "owners_before": [
        "3yfQPHeWAa1MxTX9Zf9176QqcpcnWcanVZZbaHb8B3h9"
      ]
    }
  ],
  "metadata": {
    "sequence": 2
  },
  "operation": "TRANSFER",
  "outputs": [
    {
      "amount": "1",
      "condition": {
        "details": {
          "public_key": "3Af3fhhjU6d9WecEM9Uw5hfom9kNEwE7YuDWdqAUssqm",
          "type": "ed25519-sha-256"
        },
        "uri": "ni:///sha-256;Ll1r0LzgHUvWB87yIrNFYo731MMUEypqvrbPATTbuD4?
↪fpt=ed25519-sha-256&cost=131072"
      },
      "public_keys": [
        "3Af3fhhjU6d9WecEM9Uw5hfom9kNEwE7YuDWdqAUssqm"
      ]
    }
  ],
  "version": "1.0"
```

```
}]
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – A list of transactions containing an asset with ID `asset_id` was found and returned.
- 400 Bad Request – The request wasn't understood by the server, e.g. the `asset_id` querystring was not included in the request.

`POST /api/v1/transactions`

Push a new transaction.

Note: The posted transaction should be structurally valid and not spending an already spent output. The steps to build a valid transaction are beyond the scope of this page. One would normally use a driver such as the BigchainDB Python Driver to build a valid transaction.

Example request:

```
POST /api/v1/transactions/ HTTP/1.1
Host: example.com
Content-Type: application/json

{
  "asset": {
    "data": {
      "msg": "Hello BigchainDB!"
    }
  },
  "id": "8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102",
  "inputs": [
    {
      "fulfillment": "pGSAIDE5i63cn4X8T8N1sZ2mGkJD5lNRnBM4PZgI_zvzbr-
↪cgUCGvCc2HO2uB4IKix6INRzGIM10r7VsKFMPM9cT7uVJ1xFLOJ9bn6UioepBMLIrrwTlk2CkTolIPonf7BnzriQL
↪",
      "fulfills": null,
      "owners_before": [
        "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
      ]
    }
  ],
  "metadata": {
    "sequence": 0
  },
  "operation": "CREATE",
  "outputs": [
    {
      "amount": "1",
      "condition": {
        "details": {
          "public_key": "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD",
          "type": "ed25519-sha-256"
        },
```

```
        "uri": "ni:///sha-256;PNYwdxaRaNw60N6LDFzOWO97b8tJeragczakL8PrAPc?
↪fpt=ed25519-sha-256&cost=131072"
      },
      "public_keys": [
        "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
      ]
    }
  ],
  "version": "1.0"
}
```

Example response:

```
HTTP/1.1 202 Accepted
Location: ../statuses?transaction_
↪id=8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102
Content-Type: application/json

{
  "asset": {
    "data": {
      "msg": "Hello BigchainDB!"
    }
  },
  "id": "8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102",
  "inputs": [
    {
      "fulfillment": "pGSAIDE5i63cn4X8T8N1sZ2mGkJD5lNRnBM4PZgI_zvzbr-
↪cgUCGvCc2HO2uB4IKix6INRzGIM10r7VsKFMPM9cT7uVJ1xFLOJ9bn6UioepBMLIrrwTlk2CkTolIPonf7BnzriQL
↪",
      "fulfills": null,
      "owners_before": [
        "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
      ]
    }
  ],
  "metadata": {
    "sequence": 0
  },
  "operation": "CREATE",
  "outputs": [
    {
      "amount": "1",
      "condition": {
        "details": {
          "public_key": "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD",
          "type": "ed25519-sha-256"
        },
        "uri": "ni:///sha-256;PNYwdxaRaNw60N6LDFzOWO97b8tJeragczakL8PrAPc?
↪fpt=ed25519-sha-256&cost=131072"
      },
      "public_keys": [
        "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
      ]
    }
  ],
  "version": "1.0"
}
```

Note: If the server is returning a `202` HTTP status code, then the transaction has been accepted for processing. To check the status of the transaction, poll the link to the *status monitor* provided in the `Location` header or listen to server's *WebSocket Event Stream API*.

Response Headers

- Content-Type – `application/json`
- Location – Relative link to a status monitor for the submitted transaction.

Status Codes

- 202 Accepted – The pushed transaction was accepted in the `BACKLOG`, but the processing has not been completed.
- 400 Bad Request – The transaction was malformed and not accepted in the `BACKLOG`.

8.4 Transaction Outputs

The `/api/v1/outputs` endpoint returns transactions outputs filtered by a given public key, and optionally filtered to only include either spent or unspent outputs.

`GET /api/v1/outputs`
Get transaction outputs by public key. The `public_key` parameter must be a base58 encoded ed25519 public key associated with transaction output ownership.

Returns a list of transaction outputs.

Parameters

- **`public_key`** – Base58 encoded public key associated with output ownership. This parameter is mandatory and without it the endpoint will return a `400` response code.
- **`spent`** – Boolean value ("true" or "false") indicating if the result set should include only spent or only unspent outputs. If not specified the result includes all the outputs (both spent and unspent) associated with the `public_key`.

`GET /api/v1/outputs?public_key={public_key}`

Return all outputs, both spent and unspent, for the `public_key`.

Example request:

```
GET /api/v1/outputs?public_key=1AAAbbb...ccc HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

[
  {
    "output_index": 0,
    "transaction_id":
↪"2d431073e1477f3073a4693ac7ff9be5634751de1b8abaa1f4e19548ef0b4b0e"
  },
  {
```

```
    "output_index": 1,
    "transaction_id":
↪"2d431073e1477f3073a4693ac7ff9be5634751de1b8abaa1f4e19548ef0b4b0e"
  }
]
```

Status Codes

- 200 OK – A list of outputs were found and returned in the body of the response.
- 400 Bad Request – The request wasn't understood by the server, e.g. the `public_key` querystring was not included in the request.

`GET /api/v1/outputs?public_key={public_key}&spent=true`

Return all **spent** outputs for `public_key`.

Example request:

```
GET /api/v1/outputs?public_key=1AAAbbb...ccc&spent=true HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

[
  {
    "output_index": 0,
    "transaction_id":
↪"2d431073e1477f3073a4693ac7ff9be5634751de1b8abaa1f4e19548ef0b4b0e"
  }
]
```

Status Codes

- 200 OK – A list of outputs were found and returned in the body of the response.
- 400 Bad Request – The request wasn't understood by the server, e.g. the `public_key` querystring was not included in the request.

`GET /api/v1/outputs?public_key={public_key}&spent=false`

Return all **unspent** outputs for `public_key`.

Example request:

```
GET /api/v1/outputs?public_key=1AAAbbb...ccc&spent=false HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

[
  {
    "output_index": 1,
```

```
    "transaction_id":
↪"2d431073e1477f3073a4693ac7ff9be5634751de1b8abaa1f4e19548ef0b4b0e"
  }
]
```

Status Codes

- 200 OK – A list of outputs were found and returned in the body of the response.
- 400 Bad Request – The request wasn't understood by the server, e.g. the `public_key` querystring was not included in the request.

8.5 Statuses

`GET /api/v1/statuses`
Get the status of an asynchronously written transaction or block by their id.

Query Parameters

- **`transaction_id`** (*string*) – transaction ID
- **`block_id`** (*string*) – block ID

Note: Exactly one of the `transaction_id` or `block_id` query parameters must be used together with this endpoint (see below for getting *transaction statuses* and *block statuses*).

`GET /api/v1/statuses?transaction_id={transaction_id}`

Get the status of a transaction.

The possible status values are `undecided`, `valid` or `backlog`. If a transaction in neither of those states is found, a `404 Not Found` HTTP status code is returned. We're currently looking into ways to unambigously let the user know about a transaction's status that was included in an invalid block.

Example request:

```
GET /statuses?transaction_
↪id=8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "status": "valid"
}
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – A transaction with that ID was found.

- 404 Not Found – A transaction with that ID was not found.

GET /api/v1/statuses?block_id={block_id}

Get the status of a block.

The possible status values are `undecided`, `valid` or `invalid`.

Example request:

```
GET /api/v1/statuses?block_
↪id=7f1d3932fd366fcee1458c27cdfe47a03da2e23193842e48bcac2cc805465769 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "status": "valid"
}
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – A block with that ID was found.
- 404 Not Found – A block with that ID was not found.

8.6 Assets

GET /api/v1/assets

Return all the assets that match a given text search.

Query Parameters

- **text search** (*string*) – Text search string to query.
- **limit** (*int*) – (Optional) Limit the number of returned assets. Defaults to `0` meaning return all matching assets.

Note: Currently this enpoint is only supported if the server is running MongoDB as the backend.

GET /api/v1/assets?search={text_search}

Return all assets that match a given text search. The `id` of the asset is the same `id` of the transaction that created the asset.

If no assets match the text search it returns an empty list.

If the text string is empty or the server does not support text search, a `400` is returned.

The results are sorted by text score. For more information about the behavior of text search see MongoDB text search behavior

Example request:

```
GET /api/v1/assets/?search=bigchaindb HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-type: application/json

[
    {
        "data": {"msg": "Hello BigchainDB 1!"},
        "id": "51ce82a14ca274d43e4992bbce41f6fdeb755f846e48e710a3bbb3b0cf8e4204"
    },
    {
        "data": {"msg": "Hello BigchainDB 2!"},
        "id": "b4e9005fa494d20e503d916fa87b74fe61c079afccd6e084260674159795ee31"
    },
    {
        "data": {"msg": "Hello BigchainDB 3!"},
        "id": "fa6bcb6a8fdea3dc2a860fcdc0e0c63c9cf5b25da8b02a4db4fb6a2d36d27791"
    }
]
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – The query was executed successfully.
- 400 Bad Request – The query was not executed successfully. Returned if the text string is empty or the server does not support text search.

`GET /api/v1/assets?search={text_search}&limit={n_documents}`

Return at most `n` assets that match a given text search.

If no assets match the text search it returns an empty list.

If the text string is empty or the server does not support text search, a `400` is returned.

The results are sorted by text score. For more information about the behavior of text search see MongoDB text search behavior

Example request:

```
GET /api/v1/assets/?search=bigchaindb&limit=2 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-type: application/json

[
    {
        "data": {"msg": "Hello BigchainDB 1!"},
        "id": "51ce82a14ca274d43e4992bbce41f6fdeb755f846e48e710a3bbb3b0cf8e4204"
```

```
    },
    {
        "data": {"msg": "Hello BigchainDB 2!"},
        "id": "b4e9005fa494d20e503d916fa87b74fe61c079afccd6e084260674159795ee31"
    },
]
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – The query was executed successfully.
- 400 Bad Request – The query was not executed successfully. Returned if the text string is empty or the server does not support text search.

8.7 Transaction Metadata

`GET /api/v1/metadata`

Return all the metadata that match a given text search.

Query Parameters

- **`text search`** (*`string`*) – Text search string to query.
- **`limit`** (*`int`*) – (Optional) Limit the number of returned metadata objects. Defaults to `0` meaning return all matching objects.

Note: Currently this enpoint is only supported if the server is running MongoDB as the backend.

`GET /api/v1/metadata/?search={text_search}`

Return all metadata that match a given text search. The `id` of the metadata is the same `id` of the transaction where it was defined.

If no metadata match the text search it returns an empty list.

If the text string is empty or the server does not support text search, a `400` is returned.

The results are sorted by text score. For more information about the behavior of text search see MongoDB text search behavior

Example request:

```
GET /api/v1/metadata/?search=bigchaindb HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-type: application/json

[
    {
        "metadata": {"metakey1": "Hello BigchainDB 1!"},
        "id": "51ce82a14ca274d43e4992bbce41f6fdeb755f846e48e710a3bbb3b0cf8e4204"
```

```
    },
    {
        "metadata": {"metakey2": "Hello BigchainDB 2!"},
        "id": "b4e9005fa494d20e503d916fa87b74fe61c079afccd6e084260674159795ee31"
    },
    {
        "metadata": {"metakey3": "Hello BigchainDB 3!"},
        "id": "fa6bcb6a8fdea3dc2a860fcdc0e0c63c9cf5b25da8b02a4db4fb6a2d36d27791"
    }
]
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – The query was executed successfully.
- 400 Bad Request – The query was not executed successfully. Returned if the text string is empty or the server does not support text search.

`GET /api/v1/metadata/?search={text_search}&limit={n_documents}`

Return at most `n` metadata objects that match a given text search.

If no metadata match the text search it returns an empty list.

If the text string is empty or the server does not support text search, a `400` is returned.

The results are sorted by text score. For more information about the behavior of text search see MongoDB text search behavior

Example request:

```
GET /api/v1/metadata/?search=bigchaindb&limit=2 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-type: application/json

[
    {
        "metadata": {"msg": "Hello BigchainDB 1!"},
        "id": "51ce82a14ca274d43e4992bbce41f6fdeb755f846e48e710a3bbb3b0cf8e4204"
    },
    {
        "metadata": {"msg": "Hello BigchainDB 2!"},
        "id": "b4e9005fa494d20e503d916fa87b74fe61c079afccd6e084260674159795ee31"
    },
]
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – The query was executed successfully.

- 400 Bad Request – The query was not executed successfully. Returned if the text string is empty or the server does not support text search.

8.8 Advanced Usage

The following endpoints are more advanced and meant for debugging and transparency purposes.

More precisely, the *blocks endpoint* allows you to retrieve a block by `block_id` as well the list of blocks that a certain transaction with `transaction_id` occured in (a transaction can occur in multiple `invalid` blocks until it either gets rejected or validated by the system). This endpoint gives the ability to drill down on the lifecycle of a transaction

The *votes endpoint* contains all the voting information for a specific block. So after retrieving the `block_id` for a given `transaction_id`, one can now simply inspect the votes that happened at a specific time on that block.

8.8.1 Blocks

GET /api/v1/blocks/{block_id}

Get the block with the ID `block_id`. Any blocks, be they `VALID`, `UNDECIDED` or `INVALID` will be returned. To check a block's status independently, use the *Statuses endpoint*. To check the votes on a block, have a look at the *votes endpoint*.

Parameters

- **block_id** (*hex string*) – block ID

Example request:

```
GET /api/v1/blocks/
↪7f1d3932fd366fcee1458c27cdfe47a03da2e23193842e48bcac2cc805465769 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "block": {
    "node_pubkey": "DngBurxfeNVKZWCEcDnLj1eMPAS7focUZTE5FndFGuHT",
    "timestamp": "1511290617",
    "transactions": [
      {
        "asset": {
          "data": {
            "msg": "Hello BigchainDB!"
          }
        },
        "id": "8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102",
        "inputs": [
          {
            "fulfillment": "pGSAIDE5i63cn4X8T8N1sZ2mGkJD5lNRnBM4PZgI_zvzbr-
↪cgUCGvCc2HO2uB4IKix6INRzGIM10r7VsKFMPM9cT7uVJ1xFLOJ9bn6UioepBMLIrrwTlk2CkTolIPonf7BnzriQL
↪",
            "fulfills": null,
            "owners_before": [
```

```
              "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
            ]
          }
        ],
        "metadata": {
          "sequence": 0
        },
        "operation": "CREATE",
        "outputs": [
          {
            "amount": "1",
            "condition": {
              "details": {
                "public_key": "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD",
                "type": "ed25519-sha-256"
              },
              "uri": "ni:///sha-256;PNYwdxaRaNw60N6LDFzOWO97b8tJeragczakL8PrAPc?
↪fpt=ed25519-sha-256&cost=131072"
            },
            "public_keys": [
              "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD"
            ]
          }
        ],
        "version": "1.0"
      }
    ],
    "voters": [
      "DngBurxfeNVKZWCEcDnLj1eMPAS7focUZTE5FndFGuHT"
    ]
  },
  "id": "7f1d3932fd366fcee1458c27cdfe47a03da2e23193842e48bcac2cc805465769",
  "signature":
↪"53wxrEQDYk1dXzmvNSytbCfmNVnPqPkDQaTnAe8Jf43s6ssejPxezkCvUnGTnduNUmaLjhaan1iRLi3peu6s5DzA
↪"
}
```


Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – A block with that ID was found.
- 400 Bad Request – The request wasn't understood by the server, e.g. just requesting `/blocks` without the `block_id`.
- 404 Not Found – A block with that ID was not found.

`GET /api/v1/blocks`

The unfiltered `/blocks` endpoint without any query parameters returns a *400* status code. The list endpoint should be filtered with a `transaction_id` query parameter, see the `/blocks?transaction_id={transaction_id}&status={UNDECIDED|VALID|INVALID}` *endpoint*.

Example request:

```
GET /api/v1/blocks HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 400 Bad Request
```

Status Codes

- 400 Bad Request – The request wasn't understood by the server, e.g. just requesting `/blocks` without the `block_id`.

GET /api/v1/blocks?transaction_id={transaction_id}&status={UNDECIDED|VALID|INVALID}

Retrieve a list of `block_id` with their corresponding status that contain a transaction with the ID `transaction_id`.

Any blocks, be they `UNDECIDED`, `VALID` or `INVALID` will be returned if no status filter is provided.

Note: In case no block was found, an empty list and an HTTP status code `200 OK` is returned, as the request was still successful.

Query Parameters

- **transaction_id** (*string*) – transaction ID *(required)*
- **status** (*string*) – Filter blocks by their status. One of `VALID`, `UNDECIDED` or `INVALID`.

Example request:

```
GET /api/v1/blocks?transaction_
↪id=8b20dbe164badd5ca0611b0e233aef9acce609fbca20f787fc7d926f300d0102 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

[
  "303bab77264d944bcbe0e2615a2dc0533485b78248728d493c539ecced22886f",
  "7f1d3932fd366fcee1458c27cdfe47a03da2e23193842e48bcac2cc805465769"
]
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – A list of blocks containing a transaction with ID `transaction_id` was found and returned.
- 400 Bad Request – The request wasn't understood by the server, e.g. just requesting `/blocks`, without defining `transaction_id`.

8.8.2 Votes

GET /api/v1/votes?block_id={block_id}

Retrieve a list of votes for a certain block with ID `block_id`. To check for the validity of a vote, a user of this endpoint needs to perform the following steps:

1. Check if the vote's `node_pubkey` is allowed to vote.
2. Verify the vote's signature against the vote's body (`vote.vote`) and `node_pubkey`.

Query Parameters

- **block_id** (*string*) – The block ID to filter the votes.

Example request:

```
GET /api/v1/votes?block_
↪id=7f1d3932fd366fcee1458c27cdfe47a03da2e23193842e48bcac2cc805465769 HTTP/1.1
Host: example.com
```

Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json

[{
  "node_pubkey": "DngBurxfeNVKZWCEcDnLj1eMPAS7focUZTE5FndFGuHT",
  "signature":
↪"5cFqScdB6R6WTjx9n3TbKn2L35Z63xdwYSBpevT81YJCjSV4jZrm2DZ1wHGZXDuPGZWmnVThYDPsCHCc4B19Fv9E
↪",
  "vote": {
    "invalid_reason": null,
    "is_block_valid": true,
    "previous_block":
↪"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef",
    "timestamp": "1511290617",
    "voting_for_block":
↪"7f1d3932fd366fcee1458c27cdfe47a03da2e23193842e48bcac2cc805465769"
  }
}]
```

Response Headers

- Content-Type – `application/json`

Status Codes

- 200 OK – A list of votes voting for a block with ID `block_id` was found and returned.
- 400 Bad Request – The request wasn't understood by the server, e.g. just requesting `/votes`, without defining `block_id`.

8.9 Determining the API Root URL

When you start BigchainDB Server using `bigchaindb start`, an HTTP API is exposed at some address. The default is:

`http://localhost:9984/api/v1/`

It's bound to `localhost`, so you can access it from the same machine, but it won't be directly accessible from the outside world. (The outside world could connect via a SOCKS proxy or whatnot.)

The documentation about BigchainDB Server *Configuration Settings* has a section about how to set `server.bind` so as to make the HTTP API publicly accessible.

If the API endpoint is publicly accessible, then the public API Root URL is determined as follows:

- The public IP address (like 12.34.56.78) is the public IP address of the machine exposing the HTTP API to the public internet (e.g. either the machine hosting Gunicorn or the machine running the reverse proxy such as Nginx). It's determined by AWS, Azure, Rackspace, or whoever is hosting the machine.
- The DNS hostname (like example.com) is determined by DNS records, such as an "A Record" associating example.com with 12.34.56.78
- The port (like 9984) is determined by the `server.bind` setting if Gunicorn is exposed directly to the public Internet. If a reverse proxy (like Nginx) is exposed directly to the public Internet instead, then it could expose the HTTP API on whatever port it wants to. (It should expose the HTTP API on port 9984, but it's not bound to do that by anything other than convention.)

CHAPTER 9

The Events API

9.1 The WebSocket Event Stream API

Important: The WebSocket Event Stream runs on a different port than the Web API. The default port for the Web API is *9984*, while the one for the Event Stream is *9985*.

BigchainDB provides real-time event streams over the WebSocket protocol with the Event Stream API. Connecting to an event stream from your application enables a BigchainDB node to notify you as events occur, such as new *validated transactions*.

9.1.1 Demoing the API

You may be interested in demoing the Event Stream API with the WebSocket echo test to familiarize yourself before attempting an integration.

9.1.2 Determining Support for the Event Stream API

It's a good idea to make sure that the node you're connecting with has advertised support for the Event Stream API. To do so, send a HTTP GET request to the node's *API Root Endpoint* (e.g. `http://localhost:9984/api/v1/`) and check that the response contains a `streams` property:

```
{
 ...,
 "streams": "ws://example.com:9985/api/v1/streams/valid_transactions",
 ...
}
```

9.1.3 Connection Keep-Alive

The Event Stream API supports Ping/Pong frames as descibed in RFC 6455.

Note: It might not be possible to send PING/PONG frames via web browsers because of non availability of Javascript API on different browsers to achieve the same.

9.1.4 Streams

Each stream is meant as a unidirectional communication channel, where the BigchainDB node is the only party sending messages. Any messages sent to the BigchainDB node will be ignored.

Streams will always be under the WebSocket protocol (so `ws://` or `wss://`) and accessible as extensions to the `/api/v<version>/streams/` API root URL (for example, *validated transactions* would be accessible under `/api/v1/streams/valid_transactions`). If you're running your own BigchainDB instance and need help determining its root URL, then see the page titled *Determining the API Root URL*.

All messages sent in a stream are in the JSON format.

Note: For simplicity, BigchainDB initially only provides a stream for all validated transactions. In the future, we may provide streams for other information, such as new blocks, new votes, or invalid transactions. We may also provide the ability to filter the stream for specific qualities, such as a specific `output`'s `public_key`.

If you have specific use cases that you think would fit as part of this API, feel free to reach out via Gitter or email.

Valid Transactions

`/valid_transactions`

Streams an event for any newly validated transactions. Message bodies contain the transaction's ID, associated asset ID, and containing block's ID.

Example message:

```
{
    "transaction_id": "<sha3-256 hash>",
    "asset_id": "<sha3-256 hash>",
    "block_id": "<sha3-256 hash>"
}
```

Note: Transactions in BigchainDB are validated in batches ("blocks") and will, therefore, be streamed in batches. Each block can contain up to a 1000 transactions, ordered by the time at which they were included in the block. The `/valid_transactions` stream will send these transactions in the same order that the block stored them in, but this does **NOT** guarantee that you will recieve the events in that same order.

9.2 The Event Plugin API [experimental]

Danger: The Event Plugin API is **experimental** and might change in the future.

BigchainDB implements an internal event system that allows different software components to receive updates on specific topics. The WebSocket API, for example, is a subscriber to a stream of events called `BLOCK_VALID`. Every time a block is voted valid, the WebSocket API is notified, and it sends updates to all the clients connected.

We decided to make this internal event system public, to allow developers to integrate BigchainDB with other applications, such as AMQP systems.

9.2.1 Available Events

The event types are listed in the source file `bigchaindb/events.py`.

Table 9.1: Event Types

event name	event id	description
BLOCK_VALID	1	a block has been voted valid by the network.
BLOCK_INVALID	2	a block has been voted invalid by the network.

9.2.2 Plugin Example

We developed a minimal plugin that listens to new valid blocks and prints them to the console: https://github.com/bigchaindb/events-plugin-example

9.2.3 Architecture of an Event Plugin

Creating your own plugin is really easy, and can be summarized in few steps:

1. Create a new Python package that defines the entry point `bigchaindb.events` in its `setup.py`.
2. In your entry point, define two properties:
   - `event_types`: a variable to tell BigchainDB which events your plugin is interested in. A plugin can subscribe to more than one events by combining them using the **binary or** operator, e.g. in case you want to subscribe to both valid and invalid blocks your `event_types` can be `1 | 2`.
   - `run`: a function that will process the events coming from BigchainDB.
3. Install the newly created Python package in the current environment.
4. Add the plugin name to your BigchainDB configuration.
5. (Re)start BigchainDB.

If the installation was successful, the plugin will be run in a different process. Your plugin will receive events through a `multiprocessing.Queue` object.

Note: It's your plugin's responsibility to consume it's queue.

CHAPTER 10

Drivers & Tools

10.1 Libraries and Tools Maintained by the BigchainDB Team

- Python Driver
- JavaScript / Node.js Driver
- The Transaction CLI is a command-line interface for building BigchainDB transactions. You may be able to call it from inside the language of your choice, and then use *the HTTP API* to post transactions.

10.2 Community-Driven Libraries and Tools

Note: Some of these projects are a work in progress, but may still be useful.

- Haskell transaction builder
- Go driver
- Java driver
- Ruby driver
- Ruby library for preparing/signing transactions and submitting them or querying a BigchainDB/IPDB node (MIT licensed)

CHAPTER 11

Data Models

BigchainDB stores all data in the underlying database as JSON documents (conceptually, at least). There are three main kinds:

1. Transactions, which contain assets, inputs, outputs, and other things
2. Blocks
3. Votes

This section unpacks each one in turn.

11.1 The Transaction Model

A transaction has the following structure:

```
{
    "id": "<ID of the transaction>",
    "version": "<Transaction schema version number>",
    "inputs": ["<List of inputs>"],
    "outputs": ["<List of outputs>"],
    "operation": "<String>",
    "asset": {"<Asset model; see below>"},
    "metadata": {"<Arbitrary transaction metadata>"}
}
```

Here's some explanation of the contents:

- **id**: The ID of the transaction and also the hash of the transaction (loosely speaking). See below for an explanation of how it's computed. It's also the database primary key.
- **version**: The version-number of the transaction schema. As of BigchainDB Server 1.0.0, the only allowed value is `"1.0"`.

- **inputs**: List of inputs. Each input spends/transfers a previous output by satisfying/fulfilling the crypto-conditions on that output. A CREATE transaction should have exactly one input. A TRANSFER transaction should have at least one input (i.e. 1).
- **outputs**: List of outputs. Each output indicates the crypto-conditions which must be satisfied by anyone wishing to spend/transfer that output. It also indicates the number of shares of the asset tied to that output.
- **operation**: A string indicating what kind of transaction this is, and how it should be validated. It can only be `"CREATE"`, `"TRANSFER"` or `"GENESIS"` (but there should only be one transaction whose operation is `"GENESIS"`: the one in the GENESIS block).
- **asset**: A JSON document for the asset associated with the transaction. (A transaction can only be associated with one asset.) See *the page about the asset model*.
- **metadata**: User-provided transaction metadata. It can be any valid JSON document, or `null`. **NOTE:** When using MongoDB for storage, certain restriction apply to all (including nested) keys of the `"data"` JSON document: 1) keys (i.e. key names, not values) must **not** begin with the `$` character, and 2) keys must not contain `.` or the null character (Unicode code point 0000).

How the transaction ID is computed. 1) Build a Python dictionary containing `version`, `inputs`, `outputs`, `operation`, `asset`, `metadata` and their values, 2) In each of the inputs, replace the value of each `fulfillment` with `null`, 3) *Serialize* that dictionary, 4) The transaction ID is just *the SHA3-256 hash* of the serialized dictionary.

About signing the transaction. Later, when we get to the models for the block and the vote, we'll see that both include a signature (from the node which created it). You may wonder why transactions don't have signatures... The answer is that they do! They're just hidden inside the `fulfillment` string of each input. What gets signed (as of version 1.0.0) is everything inside the transaction, including the `id`, but the value of each `fulfillment` is replaced with `null`.

There are example BigchainDB transactions in *the HTTP API documentation* and the Python Driver documentation.

11.1.1 The Transaction Schema

BigchainDB checks all transactions (JSON documents) against a formal schema defined in *some JSON Schema files named transaction.yaml, transaction_create.yaml and transaction_transfer.yaml*.

11.2 The Asset Model

To avoid redundant data in transactions, the asset model is different for `CREATE` and `TRANSFER` transactions.

11.2.1 In CREATE Transactions

In a `CREATE` transaction, the `"asset"` must contain exactly one key-value pair. The key must be `"data"` and the value can be any valid JSON document, or `null`. For example:

```
{
    "data": {
                "desc": "Gold-inlay bookmark owned by Xavier Bellomat Dickens III",
                "xbd_collection_id": 1857
            }
}
```

When using MongoDB for storage, certain restriction apply to all (including nested) keys of the `"data"` JSON document:

- Keys (i.e. key names, not values) must **not** begin with the `$` character.
- Keys must not contain `.` or the null character (Unicode code point 0000).
- The key `"language"` (at any level in the hierarchy) is a special key and used for specifying text search language. Its value must be one of the allowed values; see the valid Text Search Languages in the MongoDB Docs. In BigchainDB, only the languages supported by *MongoDB community edition* are allowed.

11.2.2 In TRANSFER Transactions

In a `TRANSFER` transaction, the `"asset"` must contain exactly one key-value pair. They key must be `"id"` and the value must contain a transaction ID (i.e. a SHA3-256 hash: the ID of the `CREATE` transaction which created the asset, which also serves as the asset ID). For example:

```
{
    "id": "38100137cea87fb9bd751e2372abb2c73e7d5bcf39d940a5516a324d9c7fb88d"
}
```

11.3 Inputs and Outputs

There's a high-level overview of inputs and outputs in the root docs page about transaction concepts.

BigchainDB is modelled around *assets*, and *inputs* and *outputs* are the mechanism by which control of an asset (or shares of an asset) is transferred. Amounts of an asset are encoded in the outputs of a transaction, and each output may be spent separately. To spend an output, the output's `condition` must be met by an `input` that provides a corresponding `fulfillment`. Each output may be spent at most once, by a single input. Note that any asset associated with an output holding an amount greater than one is considered a divisible asset that may be split up in future transactions.

11.3.1 Inputs

An input has the following structure:

```
{
    "owners_before": ["<The public_keys list in the output being spent>"],
    "fulfillment": "<String that fulfills the condition in the output being spent>",
    "fulfills": {
        "output_index": "<Index of the output being spent (an integer)>",
        "transaction_id": "<ID of the transaction containing the output being spent>"
    }
}
```

You can think of the `fulfills` object as a pointer to an output on another transaction: the output that this input is spending/transferring. A CREATE transaction should have exactly one input. That input can contain one or more `owners_before`, a `fulfillment` (with one signature from each of the owners-before), and the value of `fulfills` should be `null`). A TRANSFER transaction should have at least one input, and the value of `fulfills` should not be `null`.

The `fulfillment` string fulfills the condition in the output that is being spent (transferred). To calculate it:

1. Determine the fulfillment as per the Crypto-Conditions spec (version 02).
2. Encode the fulfillment using the ASN.1 Distinguished Encoding Rules (DER).
3. Encode the resulting bytes using "base64url" (*not* typical base64) as per RFC 4648, Section 5.

To do those calculations, you can use one of the *BigchainDB drivers or transaction-builders*, or use a low-level crypto-conditions library as illustrated in the page about Handcrafting Transactions. A `fulfillment` string should look something like:

```
"pGSAIDgbT-nnN57wgI4Cx17gFHv3UB_pIeAzwZCk10rAjs9bgUDxyNnXMl-
↪5PFgSIOrN7br2Tz59MiWe2XY0zlC7LcN52PKhpmdRtcr7GR1PXuTfQ9dE3vGhv7LHn6QqDD6qYHYM"
```

11.3.2 Outputs

An output has the following structure:

```
{
    "condition": {"<Condition object>"},
    "public_keys": ["<List of all public keys associated with the condition object>"],
    "amount": "<Number of shares of the asset (an integer in a string)>"
}
```

The *page about conditions* explains the contents of a `condition`.

The list of `public_keys` is always the "owners" of the asset at the time the transaction completed, but before the next transaction started.

Note that `amount` must be a string (e.g. `"7"`). In a TRANSFER transaction, the sum of the output amounts must be the same as the sum of the outputs that it transfers (i.e. the sum of the input amounts). For example, if a TRANSFER transaction has two outputs, one with `"amount": "2"` and one with `"amount": "3"`, then the sum of the outputs is 5 and so the sum of the outputs-being-transferred must also be 5.

Note: The BigchainDB documentation and code talks about control of an asset in terms of "owners" and "ownership." The language is chosen to represent the most common use cases, but in some more complex scenarios, it may not be accurate to say that the output is owned by the controllers of those public keys—it would only be correct to say that those public keys are associated with the ability to fulfill the conditions on the output. Also, depending on the use case, the entity controlling an output via a private key may not be the legal owner of the asset in the corresponding legal domain. However, since we aim to use language that is simple to understand and covers the majority of use cases, we talk in terms of "owners" of an output that have the ability to "spend" that output.

11.4 Conditions

At a high level, a condition is like a lock on an output. If can you satisfy the condition, you can unlock the output and transfer/spend it. BigchainDB Server supports a subset of the ILP Crypto-Conditions (version 02 of Crypto-Conditions).

A condition object can be quite elaborate, with many nested levels, but the simplest case is actually quite simple. Here's an example signature condition:

```
{
    "details": {
        "type": "ed25519-sha-256",
        "public_key": "HFp773FH21sPFrn4y8wX3Ddrkzhqy4La4cQLfePT2vz7"
    },
    "uri": "ni:///sha-256;at0MY6Ye8yvidsgL9FrnKmsVzX0XrNNXFmuAPF4bQeU?fpt=ed25519-sha-
↪256&cost=131072"
}
```

If someone wants to spend the output where this condition is found, then they must create a TRANSFER transaction with an input that fulfills it (this condition). Because it's a ed25519-sha-256 signature condition, that means they must sign the TRANSFER transaction with the private key corresponding to the public key HFp773...

11.4.1 Supported Crypto-Conditions

BigchainDB Server v1.0 supports two of the Crypto-Conditions:

1. ED25519-SHA-256 signature conditions
2. THRESHOLD-SHA-256 threshold conditions

We saw an example signature condition above. For more information about how BigchainDB handles keys and signatures, see the page titled *Signature Algorithm and Keys*.

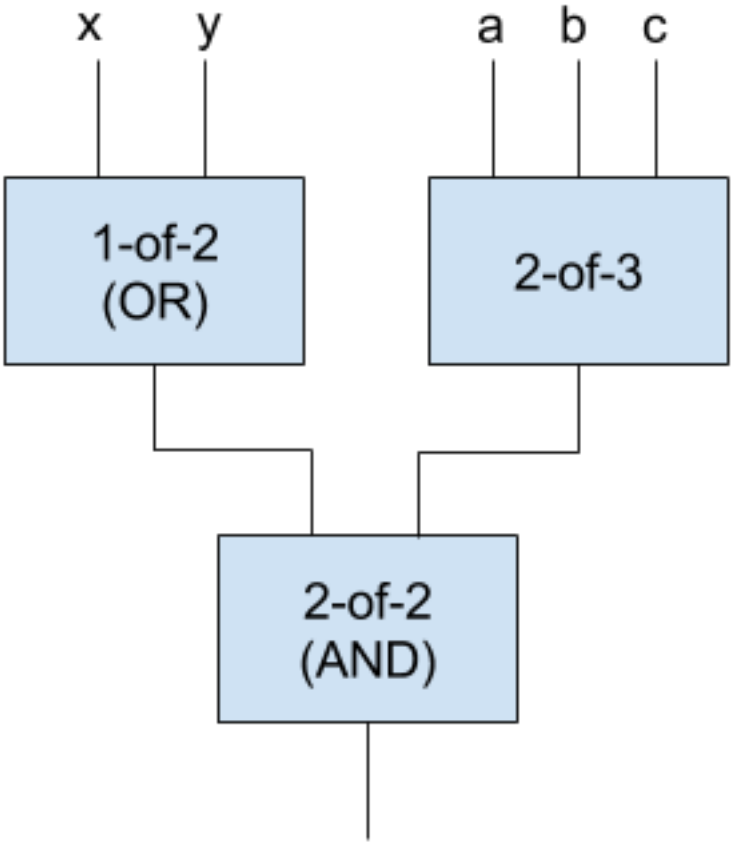
A more complex condition can be composed by using n signature conditions as inputs to an m-of-n threshold condition: a logic gate which outputs TRUE if and only if m or more inputs are TRUE. If there are n inputs to a threshold condition:

- 1-of-n is the same as a logical OR of all the inputs
- n-of-n is the same as a logical AND of all the inputs

For example, you could create a condition requiring m (of n) signatures. Here's an example 2-of-2 condition:


```
{
    "details": {
        "type": "threshold-sha-256",
        "threshold": 2,
        "subconditions": [
            {
                "public_key": "5ycPMinRx7D7e6wYXLNLa3TCtQrMQfjkap4ih7JVJy3h",
                "type": "ed25519-sha-256"
            },
            {
                "public_key": "9RSas2uCxR5sx1rJoUgcd2PB3tBK7KXuCHbUMbnH3X1M",
                "type": "ed25519-sha-256"
             }
         ]
     },
     "uri": "ni:///sha-256;zr5oThl2kk6613WKGFDg-JGu00Fv88nXcDcp6Cyr0Vw?fpt=threshold-
↪sha-256&cost=264192&subtypes=ed25519-sha-256"
}
```


The (single) output of a threshold condition can be used as one of the inputs to another threshold condition. That means you can combine threshold conditions to build complex expressions such as `(x OR y) AND (2 of {a, b, c})`.



When you create a condition, you can calculate its cost, an estimate of the resources that would be required to validate the fulfillment. For example, the cost of one signature condition is 131072. A BigchainDB federation can put an upper limit on the complexity of each condition, either directly by setting a maximum allowed cost, or indirectly by *setting a maximum allowed transaction size* which would limit the overall complexity accross all inputs and outputs of a transaction. Note: At the time of writing, there was no configuration setting to set a maximum allowed cost, so the only real option was to *set a maximum allowed transaction size*.

11.4.2 Constructing a Condition

The above examples should make it clear how to construct a condition object, but they didn't say how to generate the `uri`. If you want to generate a correct condition URI, then you should consult the Crypto-Conditions spec or use one of the existing Crypto-Conditions packages/libraries (which are used by the BigchainDB Drivers).

- Crypto-Conditions Spec (Version 02)
- BigchainDB *Drivers & Tools*

The Handcrafting Transactions page may also be of interest.

11.5 The Block Model

A block is a JSON object with a particular schema, as outlined in this page. A block must contain the following JSON keys (also called names or fields):

```
{
  "id": "<ID of the block>",
  "block": {
    "timestamp": "<Block-creation timestamp>",
    "transactions": ["<List of transactions>"],
    "node_pubkey": "<Public key of the node which created the block>",
    "voters": ["<List of public keys of all nodes in the cluster>"]
  },
  "signature": "<Signature of inner block object>"
}
```

11.5.1 The JSON Keys in a Block

id

The transaction ID and also the SHA3-256 hash of the inner `block` object, loosely speaking. It's a string. To compute it, 1) construct an *associative array* `d` containing `block.timestamp`, `block.transactions`, `block.node_pubkey`, `block.voters`, and their values. 2) compute `id = hash_of_aa(d)`. There's pseudocode for the `hash_of_aa()` function in the IPDB Protocol documentation page about cryptographic hashes. The result (`id`) is a string: the block ID. An example is `"b60adf655932bf47ef58c0bfb2dd276d4795b94346b36cbb477e10d7eb02cea8"`

block.timestamp

The Unix time when the block was created, according to the node which created it. It's a string representation of an integer. An example is `"1507294217"`.

block.transactions

A list of the *transactions* included in the block. (Each transaction is a JSON object.)

block.node_pubkey

The public key of the node that created the block. It's a string. See the IPDB Protocol documentation page about cryptographic keys & signatures.

block.voters

A list of the public keys of all cluster nodes at the time the block was created. It's a list of strings. This list can change from block to block, as nodes join and leave the cluster.

signature

The cryptographic signature of the inner `block` by the node that created the block (i.e. the node with public key `node_pubkey`). To compute that:

1. Construct an *associative array* `d` containing the contents of the inner `block` (i.e. `block.timestamp`, `block.transactions`, `block.node_pubkey`, `block.voters`, and their values).
2. Compute `signature = sig_of_aa(d, private_key)`, where `private_key` is the node's private key (i.e. `node_pubkey` and `private_key` are a key pair). There's pseudocode for the `sig_of_aa()` function on the IPDB Protocol documentation page about cryptographic keys and signatures.

Note: The `d_bytes` computed when computing the block ID will be the *same* as the `d_bytes` computed when computing the block signature. This can be used to avoid redundant calculations.

11.6 The Vote Model

A vote is a JSON object with a particular schema, as outlined in this page. A vote must contain the following JSON keys (also called names or fields):

```
{
    "node_pubkey": "<The public key of the voting node>",
    "vote": {
        "voting_for_block": "<ID of the block the node is voting on>",
        "previous_block": "<ID of the block previous to the block being voted on>",
        "is_block_valid": "<true OR false>",
        "invalid_reason": null,
        "timestamp": "<Vote-creation timestamp>"
    },
    "signature": "<Signature of inner vote object>"
}
```

Note: Votes have no ID (or `"id"`), as far as users are concerned. The backend database may use one internally, but it's of no concern to users and it's never reported to them via APIs.

11.6.1 The JSON Keys in a Vote

node_pubkey

The public key of the node which cast this vote. It's a string. For more information about public keys, see the IPDB Protocol documentation page about cryptographic keys and signatures.

vote.voting_for_block

The block ID that this vote is for. It's a string. For more information about block IDs, see the page about *blocks*.

vote.previous_block

The block ID of the block "before" the block that this vote is for, according to the node which cast this vote. It's a string. (It's possible for different nodes to see different block orders.) For more information about block IDs, see the page about *blocks*.

vote.is_block_valid

`true` if the node which cast this vote considered the block in question to be valid, and `false` otherwise. Note that it's a *boolean* (i.e. `true` or `false`), not a string.

vote.invalid_reason

Always `null`, that is, it's not being used. It may be used or dropped in a future version. See bigchaindb/bigchaindb issue #217 on GitHub.

vote.timestamp

The Unix time when the vote was created, according to the node which created it. It's a string representation of an integer.

signature

The cryptographic signature of the inner `vote` by the node that created the vote (i.e. the node with public key `node_pubkey`). To compute that:

1. Construct an *associative array* `d` containing the contents of the inner `vote` (i.e. `vote.voting_for_block`, `vote.previous_block`, `vote.is_block_valid`, `vote.invalid_reason`, `vote.timestamp`, and their values).
2. Compute `signature = sig_of_aa(d, private_key)`, where `private_key` is the node's private key (i.e. `node_pubkey` and `private_key` are a key pair). There's pseudocode for the `sig_of_aa()` function on the IPDB Protocol documentation page about cryptographic keys and signatures.

11.6.2 The Vote Schema

BigchainDB checks all votes (JSON documents) against a formal schema defined in a *JSON Schema file named vote.yaml*.

11.6.3 An Example Vote

```
{
    "node_pubkey": "3ZCsVWPAhPTqHx9wZVxp9Se54pcNeeM5mQvnozDWyDR9",
    "vote": {
        "voting_for_block":
↪"11c3a3fcc9efa4fc4332a0849fc39b58e403ff37794a7d1fdfb9e7703a94a274",
        "previous_block":
↪"3dd1441018b782a50607dc4c7f83a0f0a23eb257f4b6a8d99330dfff41271e0d",
        "is_block_valid": true,
        "invalid_reason": null,
        "timestamp": "1509977988"
    },
    "signature":
↪"3tW2EBVgxaZTE6nixVd9QEQf1vUxqPmQaNAMdCHc7zHik5KEosdkwScGYt4VhiHDTB6BCxTUzmqu3P7oP93tRWfj
↪"
}
```

CHAPTER 12

Release Notes

You can find a list of all BigchainDB Server releases and release notes on GitHub at:

https://github.com/bigchaindb/bigchaindb/releases

The CHANGELOG.md file contains much the same information, but it also has notes about what to expect in the *next* release.

We also have a roadmap document in ROADMAP.md.

CHAPTER 13

Glossary

associative array A collection of key/value (or name/value) pairs such that each possible key appears at most once in the collection. In JavaScript (and JSON), all objects behave as associative arrays with string-valued keys. In Python and .NET, associative arrays are called *dictionaries*. In Java and Go, they are called *maps*. In Ruby, they are called *hashes*. See also: Wikipedia's articles for Associative array and Comparison of programming languages (associative array)

CHAPTER 14

Appendices

14.1 How to Install OS-Level Dependencies

BigchainDB Server has some OS-level dependencies that must be installed.

On Ubuntu 16.04, we found that the following was enough:

```
sudo apt-get update
sudo apt-get install libffi-dev libssl-dev
```

On Fedora 23–25, we found that the following was enough:

```
sudo dnf update
sudo dnf install gcc-c++ redhat-rpm-config python3-devel libffi-devel
```

(If you're using a version of Fedora before version 22, you may have to use `yum` instead of `dnf`.)

14.2 How to Install the Latest pip and setuptools

You can check the version of `pip` you're using (in your current virtualenv) by doing:

```
pip -V
```

If it says that `pip` isn't installed, or it says `pip` is associated with a Python version less than 3.5, then you must install a `pip` version associated with Python 3.5+. In the following instructions, we call it `pip3` but you may be able to use `pip` if that refers to the same thing. See the `pip` installation instructions.

On Ubuntu 16.04, we found that this works:

```
sudo apt-get install python3-pip
```

That should install a Python 3 version of `pip` named `pip3`. If that didn't work, then another way to get `pip3` is to do `sudo apt-get install python3-setuptools` followed by `sudo easy_install3 pip`.

You can upgrade `pip` (`pip3`) and `setuptools` to the latest versions using:

```
pip3 install --upgrade pip setuptools
```

14.3 JSON Serialization

We needed to clearly define how to serialize a JSON object to calculate the hash.

The serialization should produce the same byte output independently of the architecture running the software. If there are differences in the serialization, hash validations will fail although the transaction is correct.

For example, consider the following two methods of serializing `{'a': 1}`:

```
# Use a serializer provided by RethinkDB
a = r.expr({'a': 1}).to_json().run(b.connection)
u'{"a":1}'

# Use the serializer in Python's json module
b = json.dumps({'a': 1})
'{"a": 1}'

a == b
False
```

The results are not the same. We want a serialization and deserialization so that the following is always true:

```
deserialize(serialize(data)) == data
True
```

Since BigchainDB performs a lot of serialization we decided to use python-rapidjson which is a python wrapper for rapidjson a fast and fully RFC complient JSON parser.

```
import rapidjson

rapidjson.dumps(data, skipkeys=False,
                ensure_ascii=False,
                sort_keys=True)
```

- `skipkeys`: With skipkeys `False` if the provided keys are not a string the serialization will fail. This way we enforce all keys to be strings
- `ensure_ascii`: The RFC recommends `utf-8` for maximum interoperability. By setting `ensure_ascii` to `False` we allow unicode characters and python-rapidjson forces the encoding to `utf-8`.
- `sort_keys`: Sorted output by keys.

Every time we need to perform some operation on the data like calculating the hash or signing/verifying the transaction, we need to use the previous criteria to serialize the data and then use the `byte` representation of the serialized data (if we treat the data as bytes we eliminate possible encoding errors e.g. unicode characters). For example:

```
# calculate the hash of a transaction
# the transaction is a dictionary
tx_serialized = bytes(serialize(tx))
tx_hash = hashlib.sha3_256(tx_serialized).hexdigest()

# signing a transaction
tx_serialized = bytes(serialize(tx))
```

```
signature = sk.sign(tx_serialized)

# verify signature
tx_serialized = bytes(serialize(tx))
pk.verify(signature, tx_serialized)
```

14.4 Cryptography

The section documents the cryptographic algorithms and Python implementations that we use.

Before hashing or computing the signature of a JSON document, we serialize it as described in the section on JSON serialization.

14.4.1 Hashes

BigchainDB computes transaction and block hashes using an implementation of the SHA3-256 algorithm provided by the **pysha3** package, which is a wrapper around the optimized reference implementation from http://keccak.noekeon.org.

Important: Since selecting the Keccak hashing algorithm for SHA-3 in 2012, NIST released a new version of the hash using the same algorithm but slightly different parameters. As of version 0.9, BigchainDB is using the latest version, supported by pysha3 1.0b1. See below for an example output of the hash function.

Here's the relevant code from 'bigchaindb/bigchaindb/common/crypto.py:

```
import sha3

def hash_data(data):
    """Hash the provided data using SHA3-256"""
    return sha3.sha3_256(data.encode()).hexdigest()
```

The incoming `data` is understood to be a Python 3 string, which may contain Unicode characters such as `'ü'` or `''`. The Python 3 `encode()` method converts `data` to a bytes object. `sha3.sha3_256(data.encode())` is a _sha3.SHA3 object; the `hexdigest()` method converts it to a hexadecimal string. For example:

```
>>> import sha3
>>> data = ''
>>> sha3.sha3_256(data.encode()).hexdigest()
'2b38731ba4ef72d4034bef49e87c381d1fbe75435163b391dd33249331f91fe7'
>>> data = 'hello world'
>>> sha3.sha3_256(data.encode()).hexdigest()
'644bcc7e564373040999aac89e7622f3ca71fba1d972fd94a31c3bfbf24e3938'
```

Note: Hashlocks (which are one kind of crypto-condition) may use a different hash function.

14.4.2 Signature Algorithm and Keys

BigchainDB uses the Ed25519 public-key signature system for generating its public/private key pairs. Ed25519 is an instance of the Edwards-curve Digital Signature Algorithm (EdDSA). As of December 2016, EdDSA was an "Internet-Draft" with the IETF but was already widely used.

BigchainDB uses the the **cryptoconditions** package to do signature and keypair-related calculations. That package, in turn, uses the **PyNaCl** package, a Python binding to the Networking and Cryptography (NaCl) library.

All keys are represented with a Base58 encoding. The cryptoconditions package uses the **base58** package to calculate a Base58 encoding. (There's no standard for Base58 encoding.) Here's an example public/private key pair:

```
"keypair": {
    "public": "9WYFf8T65bv4S8jKU8wongKPD4AmMZAwvk1absFDbYLM",
    "private": "3x7MQpPq8AEUGEuzAxSVHjU1FhLWVQJKFNNkvHhJPGCX"
}
```

14.5 The Bigchain class

The Bigchain class is the top-level Python API for BigchainDB. If you want to create and initialize a BigchainDB database, you create a Bigchain instance (object). Then you can use its various methods to create transactions, write transactions (to the object/database), read transactions, etc.

class bigchaindb.**Bigchain**(*public_key=None*, *private_key=None*, *keyring=[]*, *connection=None*, *backlog_reassign_delay=None*)

Bigchain API

Create, read, sign, write transactions to the database

__init__(*public_key=None*, *private_key=None*, *keyring=[]*, *connection=None*, *backlog_reassign_delay=None*)

Initialize the Bigchain instance

A Bigchain instance has several configuration parameters (e.g. host). If a parameter value is passed as an argument to the Bigchain __init__ method, then that is the value it will have. Otherwise, the parameter value will come from an environment variable. If that environment variable isn't set, then the value will come from the local configuration file. And if that variable isn't in the local configuration file, then the parameter will have its default value (defined in bigchaindb.__init__).

Parameters

- **public_key** (*str*) – the base58 encoded public key for the ED25519 curve.
- **private_key** (*str*) – the base58 encoded private key for the ED25519 curve.
- **keyring** (*list[str]*) – list of base58 encoded public keys of the federation nodes.
- **connection** (*Connection*) – A connection to the database.

BLOCK_INVALID = 'invalid'

return if a block has been voted invalid

BLOCK_VALID = 'valid'

return if a block is valid, or tx is in valid block

TX_VALID = 'valid'

return if a block is valid, or tx is in valid block

BLOCK_UNDECIDED = 'undecided'

return if block is undecided, or tx is in undecided block

TX_UNDECIDED = 'undecided'

return if block is undecided, or tx is in undecided block

TX_IN_BACKLOG = 'backlog'

return if transaction is in backlog

federation

Set of federation member public keys

write_transaction(*signed_transaction*)
Write the transaction to bigchain.

When first writing a transaction to the bigchain the transaction will be kept in a backlog until it has been validated by the nodes of the federation.

Parameters **signed_transaction** (*Transaction*) – transaction with the *signature* included.

Returns database response

Return type dict

reassign_transaction(*transaction*)
Assign a transaction to a new node

Parameters **transaction** (*dict*) – assigned transaction

Returns database response or None if no reassignment is possible

Return type dict

delete_transaction(**transaction_id*)
Delete a transaction from the backlog.

Parameters ***transaction_id** (*str*) – the transaction(s) to delete

Returns The database response.

get_stale_transactions()
Get a cursor of stale transactions.

Transactions are considered stale if they have been assigned a node, but are still in the backlog after some amount of time specified in the configuration

validate_transaction(*transaction*)
Validate a transaction.

Parameters **transaction** (*Transaction*) – transaction to validate.

Returns The transaction if the transaction is valid else it raises an exception describing the reason why the transaction is invalid.

is_new_transaction(*txid*, *exclude_block_id=None*)
Return True if the transaction does not exist in any VALID or UNDECIDED block. Return False otherwise.

Parameters

- **txid** (*str*) – Transaction ID
- **exclude_block_id** (*str*) – Exclude block from search

get_block(*block_id*, *include_status=False*)
Get the block with the specified *block_id* (and optionally its status)

Returns the block corresponding to *block_id* or None if no match is found.

Parameters

- **block_id** (*str*) – transaction id of the transaction to get
- **include_status** (*bool*) – also return the status of the block the return value is then a tuple: (block, status)

get_transaction(*txid*, *include_status=False*)
Get the transaction with the specified *txid* (and optionally its status)

This query begins by looking in the bigchain table for all blocks containing a transaction with the specified *txid*. If one of those blocks is valid, it returns the matching transaction from that block. Else if some of those blocks are undecided, it returns a matching transaction from one of them. If the transaction was found in invalid blocks only, or in no blocks, then this query looks for a matching transaction in the backlog table, and if it finds one there, it returns that.

Parameters

- **txid** (*str*) – transaction id of the transaction to get
- **include_status** (*bool*) – also return the status of the transaction the return value is then a tuple: (tx, status)

Returns A `Transaction` instance if the transaction was found in a valid block, an undecided block, or the backlog table, otherwise `None`. If `include_status` is `True`, also returns the transaction's status if the transaction was found.

get_status(*txid*)

Retrieve the status of a transaction with *txid* from bigchain.

Parameters **txid** (*str*) – transaction id of the transaction to query

Returns transaction status ('valid', 'undecided', or 'backlog'). If no transaction with that *txid* was found it returns *None*

Return type (string)

get_blocks_status_containing_tx(*txid*)

Retrieve block ids and statuses related to a transaction

Transactions may occur in multiple blocks, but no more than one valid block.

Parameters **txid** (*str*) – transaction id of the transaction to query

Returns A dict of blocks containing the transaction, e.g. {block_id_1: 'valid', block_id_2: 'invalid' ...}, or None

get_asset_by_id(*asset_id*)

Returns the asset associated with an asset_id.

Parameters **asset_id** (*str*) – The asset id.

Returns dict if the asset exists else None.

get_spent(*txid*, *output*)

Check if a *txid* was already used as an input.

A transaction can be used as an input for another transaction. Bigchain needs to make sure that a given *(txid, output)* is only used once.

This method will check if the *(txid, output)* has already been spent in a transaction that is in either the *VALID*, *UNDECIDED* or *BACKLOG* state.

Parameters

- **txid** (*str*) – The id of the transaction
- **output** (*num*) – the index of the output in the respective transaction

Returns The transaction (Transaction) that used the *(txid, output)* as an input else *None*

Raises

- `CriticalDoubleSpend` – If the given *(txid, output)* was spent in
- more than one valid transaction.

get_owned_ids(*owner*)
Retrieve a list of `txid` s that can be used as inputs.

Parameters **owner** (*str*) – base58 encoded public key.

Returns list of `txid` s and `output` s pointing to another transaction's condition

Return type `list` of TransactionLink

get_outputs_filtered(*owner*, *spent=None*)
Get a list of output links filtered on some criteria

Parameters

- **owner** (*str*) – base58 encoded public_key.
- **spent** (*bool*) – If `True` return only the spent outputs. If `False` return only unspent outputs. If spent is not specified (`None`) return all outputs.

Returns list of `txid` s and `output` s pointing to another transaction's condition

Return type `list` of TransactionLink

get_transactions_filtered(*asset_id*, *operation=None*)
Get a list of transactions filtered on some criteria

create_block(*validated_transactions*)
Creates a block given a list of *validated_transactions*.

Note that this method does not validate the transactions. Transactions should be validated before calling create_block.

Parameters **validated_transactions** (*list(Transaction)*) – list of validated transactions.

Returns created block.

Return type Block

validate_block(*block*)
Validate a block.

Parameters **block** (*Block*) – block to validate.

Returns The block if the block is valid else it raises and exception describing the reason why the block is invalid.

has_previous_vote(*block_id*)
Check for previous votes from this node

Parameters **block_id** (*str*) – the id of the block to check

Returns `True` if this block already has a valid vote from this node, `False` otherwise.

Return type bool

write_block(*block*)
Write a block to bigchain.

Parameters **block** (*Block*) – block to write to bigchain.

prepare_genesis_block()
Prepare a genesis block.

create_genesis_block()
Create the genesis block

Block created when bigchain is first initialized. This method is not atomic, there might be concurrency problems if multiple instances try to write the genesis block when the BigchainDB Federation is started, but it's a highly unlikely scenario.

vote(*block_id*, *previous_block_id*, *decision*, *invalid_reason=None*)
Create a signed vote for a block given the `previous_block_id` and the `decision` (valid/invalid).

Parameters

- **block_id** (*str*) – The id of the block to vote on.
- **previous_block_id** (*str*) – The id of the previous block.
- **decision** (*bool*) – Whether the block is valid or invalid.
- **invalid_reason** (*Optional[str]*) – Reason the block is invalid

write_vote(*vote*)
Write the vote to the database.

get_last_voted_block()
Returns the last block that this node voted on.

block_election_status(*block*)
Tally the votes on a block, and return the status: valid, invalid, or undecided.

get_assets(*asset_ids*)
Return a list of assets that match the asset_ids

Parameters **asset_ids** (`list` of `str`) – A list of asset_ids to retrieve from the database.

Returns The list of assets returned from the database.

Return type list

get_metadata(*txn_ids*)
Return a list of metadata that match the transaction ids (txn_ids)

Parameters **txn_ids** (`list` of `str`) – A list of txn_ids to retrieve from the database.

Returns The list of metadata returned from the database.

Return type list

write_assets(*assets*)
Writes a list of assets into the database.

Parameters **assets** (`list` of `dict`) – A list of assets to write to the database.

write_metadata(*metadata*)
Writes a list of metadata into the database.

Parameters **metadata** (`list` of `dict`) – A list of metadata to write to the database.

text_search(*search*, *, *limit=0*, *table='assets'*)
Return an iterator of assets that match the text search

Parameters

- **search** (*str*) – Text search string to query the text index
- **limit** (*int, optional*) – Limit the number of returned documents.

Returns An iterator of assets that match the text search.

Return type iter

14.6 Pipelines

14.6.1 Block Creation

This module takes care of all the logic related to block creation.

The logic is encapsulated in the `BlockPipeline` class, while the sequence of actions to do on transactions is specified in the `create_pipeline` function.

class `bigchaindb.pipelines.block.`**`BlockPipeline`**
This class encapsulates the logic to create blocks.

Note: Methods of this class will be executed in different processes.

`filter_tx`(*tx*)
Filter a transaction.

Parameters **`tx`** (*dict*) – the transaction to process.

Returns The transaction if assigned to the current node, `None` otherwise.

Return type dict

`validate_tx`(*tx*)
Validate a transaction.

Also checks if the transaction already exists in the blockchain. If it does, or it's invalid, it's deleted from the backlog immediately.

Parameters **`tx`** (*dict*) – the transaction to validate.

Returns The transaction if valid, `None` otherwise.

Return type `Transaction`

`create`(*tx*, *timeout=False*)
Create a block.

This method accumulates transactions to put in a block and outputs a block when one of the following conditions is true: - the size limit of the block has been reached, or - a timeout happened.

Parameters

- **`tx`** (`Transaction`) – the transaction to validate, might be None if a timeout happens.
- **`timeout`** (*bool*) – `True` if a timeout happened (Default: `False`).

Returns The block, if a block is ready, or `None`.

Return type `Block`

`write`(*block*)
Write the block to the Database.

Parameters **`block`** (`Block`) – the block of transactions to write to the database.

Returns The Block.

Return type `Block`

`delete_tx`(*block*)
Delete transactions.

Parameters **block** (Block) – the block containg the transactions to delete.

Returns The block.

Return type Block

bigchaindb.pipelines.block.**tx_collector**()
A helper to deduplicate transactions

bigchaindb.pipelines.block.**create_pipeline**()
Create and return the pipeline of operations to be distributed on different processes.

bigchaindb.pipelines.block.**start**()
Create, start, and return the block pipeline.

14.6.2 Block Voting

This module takes care of all the logic related to block voting.

The logic is encapsulated in the Vote class, while the sequence of actions to do on transactions is specified in the create_pipeline function.

class bigchaindb.pipelines.vote.**Vote**
This class encapsulates the logic to vote on blocks.

Note: Methods of this class will be executed in different processes.

---

ungroup(*block_id*, *transactions*)
Given a block, ungroup the transactions in it.

Parameters

- **block_id** (*str*) – the id of the block in progress.
- **transactions** (*list (dict)*) – transactions of the block in progress.

Returns None if the block has been already voted, an iterator that yields a transaction, block id, and the total number of transactions contained in the block otherwise.

validate_tx(*tx_dict*, *block_id*, *num_tx*)

Validate a transaction. Transaction must also not be in any VALID block.

Parameters

- **tx_dict** (*dict*) – the transaction to validate
- **block_id** (*str*) – the id of block containing the transaction
- **num_tx** (*int*) – the total number of transactions to process

Returns Three values are returned, the validity of the transaction, block_id, num_tx.

vote(*tx_validity*, *block_id*, *num_tx*)
Collect the validity of transactions and cast a vote when ready.

Parameters

- **tx_validity** (*bool*) – the validity of the transaction
- **block_id** (*str*) – the id of block containing the transaction
- **num_tx** (*int*) – the total number of transactions to process

Returns None, or a vote if a decision has been reached.

write_vote(*vote*, *num_tx*)
Write vote to the database.

Parameters **vote** – the vote to write.

bigchaindb.pipelines.vote.**create_pipeline**()
Create and return the pipeline of operations to be distributed on different processes.

bigchaindb.pipelines.vote.**get_changefeed**()
Create and return ordered changefeed of blocks starting from last voted block

bigchaindb.pipelines.vote.**start**()
Create, start, and return the block pipeline.

14.6.3 Block Status

This module takes care of all the logic related to block status.

Specifically, what happens when a block becomes invalid. The logic is encapsulated in the `Election` class, while the sequence of actions is specified in `create_pipeline`.

class bigchaindb.pipelines.election.**Election**(*events_queue=None*)
Election class.

check_for_quorum(*next_vote*)
Checks if block has enough invalid votes to make a decision

Parameters **next_vote** – The next vote.

requeue_transactions(*invalid_block*)
Liquidates transactions from invalid blocks so they can be processed again

14.6.4 Stale Transaction Monitoring

This module monitors for stale transactions.

It reassigns transactions which have been assigned a node but remain in the backlog past a certain amount of time.

class bigchaindb.pipelines.stale.**StaleTransactionMonitor**(*timeout=5*, *backlog_reassign_delay=None*)
This class encapsulates the logic for re-assigning stale transactions.

Note: Methods of this class will be executed in different processes.

---

check_transactions()
Poll backlog for stale transactions

Returns txs to be re assigned

Return type txs (list)

reassign_transactions(*tx*)
Put tx back in backlog with new assignee

Returns transaction

bigchaindb.pipelines.stale.**create_pipeline**(*timeout=5*, *backlog_reassign_delay=5*)
Create and return the pipeline of operations to be distributed on different processes.

bigchaindb.pipelines.stale.**start**(*timeout=5*, *backlog_reassign_delay=None*)
Create, start, and return the block pipeline.

14.7 Database Backend Interfaces

Generic backend database interfaces expected by BigchainDB.

The interfaces in this module allow BigchainDB to be agnostic about its database backend. One can configure BigchainDB to use different databases as its data store by setting the `database.backend` property in the configuration or the `BIGCHAINDB_DATABASE_BACKEND` environment variable.

14.7.1 Generic Interfaces

bigchaindb.backend.connection

bigchaindb.backend.connection.**connect**(*backend=None*, *host=None*, *port=None*, *name=None*, *max_tries=None*, *connection_timeout=None*, *replicaset=None*, *ssl=None*, *login=None*, *password=None*, *ca_cert=None*, *certfile=None*, *keyfile=None*, *keyfile_passphrase=None*, *crlfile=None*)
Create a new connection to the database backend.

All arguments default to the current configuration's values if not given.

Parameters

- **backend** (*str*) – the name of the backend to use.
- **host** (*str*) – the host to connect to.
- **port** (*int*) – the port to connect to.
- **name** (*str*) – the name of the database to use.
- **replicaset** (*str*) – the name of the replica set (only relevant for MongoDB connections).

Returns An instance of *Connection* based on the given (or defaulted) `backend`.

Raises

- `ConnectionError` – If the connection to the database fails.
- `ConfigurationError` – If the given (or defaulted) `backend` is not supported or could not be loaded.
- `AuthenticationError` – If there is a OperationFailure due to Authentication failure after connecting to the database.

class bigchaindb.backend.connection.**Connection**(*host=None*, *port=None*, *dbname=None*, *connection_timeout=None*, *max_tries=None*, ***kwargs*)
Connection class interface.

All backend implementations should provide a connection class that inherits from and implements this class.

__init__(*host=None*, *port=None*, *dbname=None*, *connection_timeout=None*, *max_tries=None*, ***kwargs*)
Create a new *Connection* instance.

Parameters

- **host** (*str*) – the host to connect to.
- **port** (*int*) – the port to connect to.
- **dbname** (*str*) – the name of the database to use.
- **connection_timeout** (*int, optional*) – the milliseconds to wait until timing out the database connection attempt. Defaults to 5000ms.
- **max_tries** (*int, optional*) – how many tries before giving up, if 0 then try forever. Defaults to 3.
- ****kwargs** – arbitrary keyword arguments provided by the configuration's `database` settings

run(*query*)

Run a query.

Parameters **query** – the query to run

Raises

- `DuplicateKeyError` – If the query fails because of a duplicate key constraint.
- `OperationFailure` – If the query fails for any other reason.
- `ConnectionError` – If the connection to the database fails.

connect()

Try to connect to the database.

Raises `ConnectionError` – If the connection to the database fails.

bigchaindb.backend.changefeed

Changefeed interfaces for backends.

class bigchaindb.backend.changefeed.**ChangeFeed**(*table*, *operation*, ***, *prefeed=None*, *connection=None*)

Create a new changefeed.

It extends `multipipes.Node` to make it pluggable in other Pipelines instances, and makes usage of `self.outqueue` to output the data.

A changefeed is a real time feed on inserts, updates, and deletes, and is volatile. This class is a helper to create changefeeds. Moreover, it provides a way to specify a `prefeed` of iterable data to output before the actual changefeed.

run_forever()

Main loop of the `multipipes.Node`

This method is responsible for first feeding the prefeed to the outqueue and after that starting the changefeed and recovering from any errors that may occur in the backend.

run_changefeed()

Backend specific method to run the changefeed.

The changefeed is usually a backend cursor that is not closed when all the results are exausted. Instead it remains open waiting for new results.

This method should also filter each result based on the `operation` and put all matching results on the outqueue of `multipipes.Node`.

bigchaindb.backend.changefeed.**get_changefeed**(*connection*, *table*, *operation*, *, *prefeed=None*)

Return a ChangeFeed.

Parameters

- **connection** (*Connection*) – A connection to the database.
- **table** (*str*) – name of the table to listen to for changes.
- **operation** (*int*) – can be ChangeFeed.INSERT, ChangeFeed.DELETE, or ChangeFeed.UPDATE. Combining multiple operation is possible with the bitwise `|` operator (e.g. `ChangeFeed.INSERT | ChangeFeed.UPDATE`)
- **prefeed** (*iterable*) – whatever set of data you want to be published first.

bigchaindb.backend.query

Query interfaces for backends.

bigchaindb.backend.query.**write_transaction**(*connection*, *signed_transaction*)

Write a transaction to the backlog table.

Parameters **signed_transaction** (*dict*) – a signed transaction.

Returns The result of the operation.

bigchaindb.backend.query.**update_transaction**(*connection*, *transaction_id*, *doc*)

Update a transaction in the backlog table.

Parameters

- **transaction_id** (*str*) – the id of the transaction.
- **doc** (*dict*) – the values to update.

Returns The result of the operation.

bigchaindb.backend.query.**delete_transaction**(*connection*, **transaction_id*)

Delete a transaction from the backlog.

Parameters ***transaction_id** (*str*) – the transaction(s) to delete.

Returns The database response.

bigchaindb.backend.query.**get_stale_transactions**(*connection*, *reassign_delay*)

Get a cursor of stale transactions.

Transactions are considered stale if they have been assigned a node, but are still in the backlog after some amount of time specified in the configuration.

Parameters **reassign_delay** (*int*) – threshold (in seconds) to mark a transaction stale.

Returns A cursor of transactions.

bigchaindb.backend.query.**get_transaction_from_block**(*connection*, *transaction_id*, *block_id*)

Get a transaction from a specific block.

Parameters

- **transaction_id** (*str*) – the id of the transaction.
- **block_id** (*str*) – the id of the block.

Returns The matching transaction.

bigchaindb.backend.query.**get_transaction_from_backlog**(*connection*, *transaction_id*)
Get a transaction from backlog.

Parameters **transaction_id** (*str*) – the id of the transaction.

Returns The matching transaction.

bigchaindb.backend.query.**get_blocks_status_from_transaction**(*connection*, *transaction_id*)
Retrieve block election information given a secondary index and value.

Parameters

- **value** – a value to search (e.g. transaction id string, payload hash string)
- **index** (*str*) – name of a secondary index, e.g. 'transaction_id'

Returns A list of blocks with with only election information

Return type list of dict

bigchaindb.backend.query.**get_asset_by_id**(*conneciton*, *asset_id*)
Returns the asset associated with an asset_id.

Parameters **asset_id** (*str*) – The asset id.

Returns Returns a rethinkdb cursor.

bigchaindb.backend.query.**get_spent**(*connection*, *transaction_id*, *condition_id*)
Check if a *txid* was already used as an input.

A transaction can be used as an input for another transaction. Bigchain needs to make sure that a given *txid* is only used once.

Parameters

- **transaction_id** (*str*) – The id of the transaction.
- **condition_id** (*int*) – The index of the condition in the respective transaction.

Returns The transaction that used the *txid* as an input else *None*

bigchaindb.backend.query.**get_spending_transactions**(*connection*, *inputs*)
Return transactions which spend given inputs

Parameters **inputs** (*list*) – list of {txid, output}

Returns Iterator of (block_ids, transaction) for transactions that spend given inputs.

bigchaindb.backend.query.**get_owned_ids**(*connection*, *owner*)
Retrieve a list of *txids* that can we used has inputs.

Parameters **owner** (*str*) – base58 encoded public key.

Returns Iterator of (block_id, transaction) for transactions that list given owner in conditions.

bigchaindb.backend.query.**get_votes_by_block_id**(*connection*, *block_id*)
Get all the votes casted for a specific block.

Parameters **block_id** (*str*) – the block id to use.

Returns A cursor for the matching votes.

bigchaindb.backend.query.**get_votes_by_block_id_and_voter**(*connection*, *block_id*, *node_pubkey*)
Get all the votes casted for a specific block by a specific voter.

Parameters

- **block_id** (*str*) – the block id to use.
- **node_pubkey** (*str*) – base58 encoded public key

Returns A cursor for the matching votes.

bigchaindb.backend.query.**get_votes_for_blocks_by_voter**(*connection*, *block_ids*, *pubkey*)

Return votes for many block_ids

Parameters

- **block_ids** (*set*) – block_ids
- **pubkey** (*str*) – public key of voting node

Returns A cursor of votes matching given block_ids and public key

bigchaindb.backend.query.**write_block**(*connection*, *block*)

Write a block to the bigchain table.

Parameters **block** (*dict*) – the block to write.

Returns The database response.

bigchaindb.backend.query.**get_block**(*connection*, *block_id*)

Get a block from the bigchain table.

Parameters **block_id** (*str*) – block id of the block to get

Returns the block or *None*

Return type *block* (dict)

bigchaindb.backend.query.**write_assets**(*connection*, *assets*)

Write a list of assets to the assets table.

Parameters **assets** (*list*) – a list of assets to write.

Returns The database response.

bigchaindb.backend.query.**write_metadata**(*connection*, *metadata*)

Write a list of metadata to the metadata table.

Parameters **metadata** (*list*) – a list of metadata to write.

Returns The database response.

bigchaindb.backend.query.**get_assets**(*connection*, *asset_ids*)

Get a list of assets from the assets table.

Parameters

- **asset_ids** (*list*) – a list of ids for the assets to be retrieved from
- **database.** (*the*) –

Returns the list of returned assets.

Return type assets (list)

bigchaindb.backend.query.**get_metadata**(*connection*, *txn_ids*)

Get a list of metadata from the metadata table.

Parameters

- **txn_ids** (*list*) – a list of ids for the metadata to be retrieved from
- **database.** (*the*) –

Returns the list of returned metadata.

Return type metadata (list)

bigchaindb.backend.query.**count_blocks**(*connection*)
Count the number of blocks in the bigchain table.

Returns The number of blocks.

bigchaindb.backend.query.**count_backlog**(*connection*)
Count the number of transactions in the backlog table.

Returns The number of transactions in the backlog.

bigchaindb.backend.query.**write_vote**(*connection*, *vote*)
Write a vote to the votes table.

Parameters **vote** (*dict*) – the vote to write.

Returns The database response.

bigchaindb.backend.query.**get_genesis_block**(*connection*)
Get the genesis block.

Returns The genesis block

bigchaindb.backend.query.**get_last_voted_block_id**(*connection*, *node_pubkey*)
Get the last voted block for a specific node.

Parameters **node_pubkey** (*str*) – base58 encoded public key.

Returns The id of the last block the node has voted on. If the node didn't cast any vote then the genesis block id is returned.

bigchaindb.backend.query.**get_txids_filtered**(*connection*, *asset_id*, *operation=None*)
Return all transactions for a particular asset id and optional operation.

Parameters

- **asset_id** (*str*) – ID of transaction that defined the asset
- **operation** (*str) (optional*) – Operation to filter on

bigchaindb.backend.query.**get_new_blocks_feed**(*connection*, *start_block_id*)
Return a generator that yields change events of the blocks feed

Parameters **start_block_id** (*str*) – ID of block to resume from

Returns Generator of change events

bigchaindb.backend.query.**text_search**(*conn*, *search*, *, *language='english'*, *case_sensitive=False*, *diacritic_sensitive=False*, *text_score=False*, *limit=0*, *table=None*)
Return all the assets that match the text search.

The results are sorted by text score. For more information about the behavior of text search on MongoDB see https://docs.mongodb.com/manual/reference/operator/query/text/#behavior

Parameters

- **search** (*str*) – Text search string to query the text index
- **language** (*str, optional*) – The language for the search and the rules for stemmer and tokenizer. If the language is `None` text search uses simple tokenization and no stemming.
- **case_sensitive** (*bool, optional*) – Enable or disable case sensitive search.

- **diacritic_sensitive** (*bool, optional*) – Enable or disable case sensitive diacritic search.
- **text_score** (*bool, optional*) – If `True` returns the text score with each document.
- **limit** (*int, optional*) – Limit the number of returned documents.

Returns a list of assets

Return type `list` of `dict`

Raises `OperationError` – If the backend does not support text search

bigchaindb.backend.schema

Database creation and schema-providing interfaces for backends.

bigchaindb.backend.schema.**TABLES**
tuple – The three standard tables BigchainDB relies on:

- `backlog` for incoming transactions awaiting to be put into a block.
- `bigchain` for blocks.
- `votes` to store votes for each block by each federation node.

bigchaindb.backend.schema.**create_database**(*connection*, *dbname*)
Create database to be used by BigchainDB.

Parameters **dbname** (*str*) – the name of the database to create.

Raises `DatabaseAlreadyExists` – If the given `dbname` already exists as a database.

bigchaindb.backend.schema.**create_tables**(*connection*, *dbname*)
Create the tables to be used by BigchainDB.

Parameters **dbname** (*str*) – the name of the database to create tables for.

bigchaindb.backend.schema.**create_indexes**(*connection*, *dbname*)
Create the indexes to be used by BigchainDB.

Parameters **dbname** (*str*) – the name of the database to create indexes for.

bigchaindb.backend.schema.**drop_database**(*connection*, *dbname*)
Drop the database used by BigchainDB.

Parameters **dbname** (*str*) – the name of the database to drop.

Raises `DatabaseDoesNotExist` – If the given `dbname` does not exist as a database.

bigchaindb.backend.schema.**init_database**(*connection=None*, *dbname=None*)
Initialize the configured backend for use with BigchainDB.

Creates a database with `dbname` with any required tables and supporting indexes.

Parameters

- **connection** (*Connection*) – an existing connection to use to initialize the database. Creates one if not given.
- **dbname** (*str*) – the name of the database to create. Defaults to the database name given in the BigchainDB configuration.

Raises `DatabaseAlreadyExists` – If the given `dbname` already exists as a database.

bigchaindb.backend.schema.**validate_language_key**(*obj*, *key*)
Validate all nested "language" key in *obj*.

Parameters **obj** (*dict*) – dictionary whose "language" key is to be validated.

Returns validation successful

Return type

None

Raises: ValidationError: will raise exception in case language is not valid.

bigchaindb.backend.schema.**validate_language**(*value*)
Check if *value* is a valid language. https://docs.mongodb.com/manual/reference/text-search-languages/

Args: value (str): language to validated

Returns: None: validation successful

Raises: ValidationError: will raise exception in case language is not valid.

bigchaindb.backend.admin

Database configuration functions.

bigchaindb.backend.utils

exception bigchaindb.backend.utils.**ModuleDispatchRegistrationError**
Raised when there is a problem registering dispatched functions for a module

14.7.2 RethinkDB Backend

RethinkDB backend implementation.

Contains a RethinkDB-specific implementation of the *changefeed*, *query*, and *schema* interfaces.

You can specify BigchainDB to use RethinkDB as its database backend by either setting `database.backend` to `'rethinkdb'` in your configuration file, or setting the `BIGCHAINDB_DATABASE_BACKEND` environment variable to `'rethinkdb'`.

If configured to use RethinkDB, BigchainDB will automatically return instances of `RethinkDBConnection` for *connect()* and dispatch calls of the generic backend interfaces to the implementations in this module.

bigchaindb.backend.rethinkdb.connection

class bigchaindb.backend.rethinkdb.connection.**RethinkDBConnection**(*host=None*, *port=None*, *dbname=None*, *connection_timeout=None*, *max_tries=None*, ***kwargs*)
This class is a proxy to run queries against the database, it is:

- lazy, since it creates a connection only when needed
- resilient, because before raising exceptions it tries more times to run the query or open a connection.

run(*query*)
Run a RethinkDB query.

Parameters **query** – the RethinkDB query.

Raises `rethinkdb.ReqlDriverError` – After `max_tries`.

bigchaindb.backend.rethinkdb.schema

bigchaindb.backend.rethinkdb.query

bigchaindb.backend.rethinkdb.query.**unwind_block_transactions**(*block*)
Yield a block for each transaction in given block

bigchaindb.backend.rethinkdb.changefeed

class bigchaindb.backend.rethinkdb.changefeed.**RethinkDBChangeFeed**(*table*, *operation*, *, *prefeed=None*, *connection=None*)
This class wraps a RethinkDB changefeed as a multipipes Node.

bigchaindb.backend.rethinkdb.changefeed.**run_changefeed**(*connection*, *table*)
Encapsulate operational logic of tailing changefeed from RethinkDB

bigchaindb.backend.rethinkdb.changefeed.**get_changefeed**(*connection*, *table*, *operation*, *, *prefeed=None*)
Return a RethinkDB changefeed.

Returns An instance of `RethinkDBChangeFeed`.

bigchaindb.backend.rethinkdb.admin

Database configuration functions.

bigchaindb.backend.rethinkdb.admin.**get_config**(*connection*, *, *table*)
Get the configuration of the given table.

Parameters

- **connection** (*Connection*) – A connection to the database.
- **table** (*str*) – The name of the table to get the configuration for.

Returns The configuration of the given table

Return type dict

bigchaindb.backend.rethinkdb.admin.**reconfigure**(*connection*, *, *table*, *shards*, *replicas*, *primary_replica_tag=None*, *dry_run=False*, *nonvoting_replica_tags=None*)
Reconfigures the given table.

Parameters

- **connection** (*Connection*) – A connection to the database.
- **table** (*str*) – The name of the table to reconfigure.

- **shards** (*int*) – The number of shards, an integer from 1-64.
- **replicas** (int | dict) –
  - If replicas is an integer, it specifies the number of replicas per shard. Specifying more replicas than there are servers will return an error.
  - If replicas is a dictionary, it specifies key-value pairs of server tags and the number of replicas to assign to those servers:

```
{'africa': 2, 'asia': 4, 'europe': 2, ...}
```

- **primary_replica_tag** (*str*) – The primary server specified by its server tag. Required if `replicas` is a dictionary. The tag must be in the `replicas` dictionary. This must not be specified if `replicas` is an integer. Defaults to `None`.
- **dry_run** (*bool*) – If `True` the generated configuration will not be applied to the table, only returned. Defaults to `False`.
- **nonvoting_replica_tags** (`list` of `str`) – Replicas with these server tags will be added to the `nonvoting_replicas` list of the resulting configuration. Defaults to `None`.

Returns

A dictionary with possibly three keys:

- `reconfigured`: the number of tables reconfigured. This will be `0` if `dry_run` is `True`.
- `config_changes`: a list of new and old table configuration values.
- `status_changes`: a list of new and old table status values.

For more information please consult RethinkDB's documentation ReQL command: reconfigure.

Return type dict

Raises `OperationError` – If the reconfiguration fails due to a RethinkDB `ReqlOpFailedError` or `ReqlQueryLogicError`.

bigchaindb.backend.rethinkdb.admin.**set_shards**(*connection*, *, *shards*, *dry_run=False*)

Sets the shards for the tables *TABLES*.

Parameters

- **connection** (*Connection*) – A connection to the database.
- **shards** (*int*) – The number of shards, an integer from 1-64.
- **dry_run** (*bool*) – If `True` the generated configuration will not be applied to the table, only returned. Defaults to `False`.

Returns

A dictionary with the configuration and status changes. For more details please see *reconfigure()*.

Return type dict

bigchaindb.backend.rethinkdb.admin.**set_replicas**(*connection*, *, *replicas*, *dry_run=False*)

Sets the replicas for the tables *TABLES*.

Parameters

- **connection** (*Connection*) – A connection to the database.
- **replicas** (*int*) – The number of replicas per shard. Specifying more replicas than there are servers will return an error.
- **dry_run** (*bool*) – If `True` the generated configuration will not be applied to the table, only returned. Defaults to `False`.

Returns

A dictionary with the configuration and status changes. For more details please see *reconfigure()*.

Return type dict

14.7.3 MongoDB Backend

Stay tuned!

14.8 Command Line Interface

14.8.1 bigchaindb.commands.bigchaindb

Implementation of the *bigchaindb* command, the command-line interface (CLI) for BigchainDB Server.

bigchaindb.commands.bigchaindb.**run_show_config**(*args*)
Show the current configuration

bigchaindb.commands.bigchaindb.**run_configure**(*args*, *skip_if_exists=False*)
Run a script to configure the current node.

Parameters **skip_if_exists** (*bool*) – skip the function if a config file already exists

bigchaindb.commands.bigchaindb.**run_export_my_pubkey**(*args*)
Export this node's public key to standard output

bigchaindb.commands.bigchaindb.**run_init**(*args*)
Initialize the database

bigchaindb.commands.bigchaindb.**run_drop**(*args*)
Drop the database

bigchaindb.commands.bigchaindb.**run_start**(*args*)
Start the processes to run the node

14.8.2 bigchaindb.commands.utils

Utility functions and basic common arguments for `argparse.ArgumentParser`.

bigchaindb.commands.utils.**configure_bigchaindb**(*command*)
Decorator to be used by command line functions, such that the configuration of bigchaindb is performed before the execution of the command.

Parameters **command** – The command to decorate.

Returns The command wrapper function.

bigchaindb.commands.utils.**start_logging_process**(*command*)
Decorator to start the logging subscriber process.

Parameters **command** – The command to decorate.

Returns The command wrapper function.

Important: Configuration, if needed, should be applied before invoking this decorator, as starting the subscriber process for logging will configure the root logger for the child process based on the state of `bigchaindb.config` at the moment this decorator is invoked.

---

bigchaindb.commands.utils.**input_on_stderr**(*prompt=''*, *default=None*, *convert=None*)
Output a string to stderr and wait for input.

Parameters

- **prompt** (*str*) – the message to display.
- **default** – the default value to return if the user leaves the field empty
- **convert** (*callable*) – a callable to be used to convert the value the user inserted. If None, the type of `default` will be used.

bigchaindb.commands.utils.**start_rethinkdb**()
Start RethinkDB as a child process and wait for it to be available.

Raises *:class:'~bigchaindb.common.exceptions.StartupError' if* – RethinkDB cannot be started.

bigchaindb.commands.utils.**start**(*parser*, *argv*, *scope*)
Utility function to execute a subcommand.

The function will look up in the `scope` if there is a function called `run_<parser.args.command>` and will run it using `parser.args` as first positional argument.

Parameters

- **parser** – an ArgumentParser instance.
- **argv** – the list of command line arguments without the script name.
- **scope** (*dict*) – map containing (eventually) the functions to be called.

Raises `NotImplementedError` – if `scope` doesn't contain a function called `run_<parser.args.command>`.

bigchaindb.commands.utils.**mongodb_host**(*host*)
Utility function that works as a type for mongodb `host` args.

This function validates the `host` args provided by to the `add-replicas` and `remove-replicas` commands and checks if each arg is in the form "host:port"

Parameters **host** (*str*) – A string containing hostname and port (e.g. "host:port")

Raises `ArgumentTypeError` – if it fails to parse the argument

14.9 Basic AWS Setup

Before you can deploy anything on AWS, you must do a few things.

14.9.1 Get an AWS Account

If you don't already have an AWS account, you can sign up for one for free at aws.amazon.com.

14.9.2 Install the AWS Command-Line Interface

To install the AWS Command-Line Interface (CLI), just do:

```
pip install awscli
```

14.9.3 Create an AWS Access Key

The next thing you'll need is AWS access keys (access key ID and secret access key). If you don't have those, see the AWS documentation about access keys.

You should also pick a default AWS region name (e.g. `eu-central-1`). That's where your cluster will run. The AWS documentation has a list of them.

Once you've got your AWS access key, and you've picked a default AWS region name, go to a terminal session and enter:

```
aws configure
```

and answer the four questions. For example:

```
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: eu-central-1
Default output format [None]: [Press Enter]
```

This writes two files: `~/.aws/credentials` and `~/.aws/config`. AWS tools and packages look for those files.

14.9.4 Generate an RSA Key Pair for SSH

Eventually, you'll have one or more instances (virtual machines) running on AWS and you'll want to SSH to them. To do that, you need a public/private key pair. The public key will be sent to AWS, and you can tell AWS to put it in any instances you provision there. You'll keep the private key on your local workstation.

See the page about how to generate a key pair for SSH.

14.9.5 Send the Public Key to AWS

To send the public key to AWS, use the AWS Command-Line Interface:

```
aws ec2 import-key-pair \
--key-name "<key-name>" \
--public-key-material file://~/.ssh/<key-name>.pub
```

If you're curious why there's a `file://` in front of the path to the public key, see issue aws/aws-cli#41 on GitHub.

If you want to verify that your key pair was imported by AWS, go to the Amazon EC2 console, select the region you gave above when you did `aws configure` (e.g. eu-central-1), click on **Key Pairs** in the left sidebar, and check that `<key-name>` is listed.

14.10 Deploy a RethinkDB-Based Testing Cluster on AWS

This section explains a way to deploy a *RethinkDB-based* cluster of BigchainDB nodes on Amazon Web Services (AWS) for testing purposes.

14.10.1 Why?

Why would anyone want to deploy a centrally-controlled BigchainDB cluster? Isn't BigchainDB supposed to be decentralized, where each node is controlled by a different person or organization?

Yes! These scripts are for deploying a testing cluster, not a production cluster.

14.10.2 How?

We use some Bash and Python scripts to launch several instances (virtual servers) on Amazon Elastic Compute Cloud (EC2). Then we use Fabric to install RethinkDB and BigchainDB on all those instances.

14.10.3 Python Setup

The instructions that follow have been tested on Ubuntu 16.04. Similar instructions should work on similar Linux distros.

Note: Our Python scripts for deploying to AWS use Python 2 because Fabric doesn't work with Python 3.

You must install the Python package named `fabric`, but it depends on the `cryptography` package, and that depends on some OS-level packages. On Ubuntu 16.04, you can install those OS-level packages using:

```
sudo apt-get install build-essential libssl-dev libffi-dev python-dev
```

For other operating systems, see the installation instructions for the `cryptography` package.

Maybe create a Python 2 virtual environment and activate it. Then install the following Python packages (in that virtual environment):

```
pip install fabric fabtools requests boto3 awscli
```

What did you just install?

- "Fabric is a Python (2.5-2.7) library and command-line tool for streamlining the use of SSH for application deployment or systems administration tasks."
- fabtools are "tools for writing awesome Fabric files"
- requests is a Python package/library for sending HTTP requests
- "Boto is the Amazon Web Services (AWS) SDK for Python, which allows Python developers to write software that makes use of Amazon services like S3 and EC2." (`boto3` is the name of the latest Boto package.)
- The aws-cli package, which is an AWS Command Line Interface (CLI).

14.10.4 Setting up in AWS

See the page about basic AWS Setup in the Appendices.

14.10.5 Get Enough Amazon Elastic IP Addresses

The AWS cluster deployment scripts use elastic IP addresses (although that may change in the future). By default, AWS accounts get five elastic IP addresses. If you want to deploy a cluster with more than five nodes, then you will need more than five elastic IP addresses; you may have to apply for those; see the AWS documentation on elastic IP addresses.

14.10.6 Create an Amazon EC2 Security Group

Go to the AWS EC2 Console and select "Security Groups" in the left sidebar. Click the "Create Security Group" button. You can name it whatever you like. (Notes: The default name in the example AWS deployment configuration file is `bigchaindb`. We had problems with names containing dashes.) The description should be something to help you remember what the security group is for.

For a super lax, somewhat risky, anything-can-enter security group, add these rules for Inbound traffic:

- Type = All TCP, Protocol = TCP, Port Range = 0-65535, Source = 0.0.0.0/0
- Type = SSH, Protocol = SSH, Port Range = 22, Source = 0.0.0.0/0
- Type = All UDP, Protocol = UDP, Port Range = 0-65535, Source = 0.0.0.0/0
- Type = All ICMP, Protocol = ICMP, Port Range = 0-65535, Source = 0.0.0.0/0

(Note: Source = 0.0.0.0/0 is CIDR notation for "allow this traffic to come from *any* IP address.")

If you want to set up a more secure security group, see the Notes for Firewall Setup.

14.10.7 Deploy a BigchainDB Cluster

Step 1

Suppose *N* is the number of nodes you want in your BigchainDB cluster. If you already have a set of *N* BigchainDB configuration files in the `deploy-cluster-aws/confiles` directory, then you can jump to the next step. To create such a set, you can do something like:

```
# in a Python 3 virtual environment where bigchaindb is installed
cd bigchaindb
cd deploy-cluster-aws
./make_confiles.sh confiles 3
```

That will create three (3) *default* BigchainDB configuration files in the `deploy-cluster-aws/confiles` directory (which will be created if it doesn't already exist). The three files will be named `bcdb_conf0`, `bcdb_conf1`, and `bcdb_conf2`.

You can look inside those files if you're curious. For example, the default keyring is an empty list. Later, the deployment script automatically changes the keyring of each node to be a list of the public keys of all other nodes. Other changes are also made. That is, the configuration files generated in this step are *not* what will be sent to the deployed nodes; they're just a starting point.

Step 2

Step 2 is to make an AWS deployment configuration file, if necessary. There's an example AWS configuration file named `example_deploy_conf.py`. It has many comments explaining each setting. The settings in that file are (or should be):

```
NUM_NODES=3
BRANCH="master"
SSH_KEY_NAME="not-set-yet"
USE_KEYPAIRS_FILE=False
IMAGE_ID="ami-8504fdea"
INSTANCE_TYPE="t2.medium"
SECURITY_GROUP="bigchaindb"
USING_EBS=True
EBS_VOLUME_SIZE=30
EBS_OPTIMIZED=False
ENABLE_WEB_ADMIN=True
BIND_HTTP_TO_LOCALHOST=True
```

Make a copy of that file and call it whatever you like (e.g. `cp example_deploy_conf.py my_deploy_conf.py`). You can leave most of the settings at their default values, but you must change the value of `SSH_KEY_NAME` to the name of your private SSH key. You can do that with a text editor. Set `SSH_KEY_NAME` to the name you used for `<key-name>` when you generated an RSA key pair for SSH (in basic AWS setup).

You'll also want to change the `IMAGE_ID` to one that's up-to-date and available in your AWS region. If you don't remember your AWS region, then look in your `$HOME/.aws/config` file. You can find an up-to-date Ubuntu image ID for your region at https://cloud-images.ubuntu.com/locator/ec2/. An example search string is "eu-central-1 16.04 LTS amd64 hvm:ebs-ssd". You should replace "eu-central-1" with your region name.

If you want your nodes to have a predictable set of pre-generated keypairs, then you should 1) set `USE_KEYPAIRS_FILE=True` in the AWS deployment configuration file, and 2) provide a `keypairs.py` file containing enough keypairs for all of your nodes. You can generate a `keypairs.py` file using the `write_keypairs_file.py` script. For example:

```
# in a Python 3 virtual environment where bigchaindb is installed
cd bigchaindb
cd deploy-cluster-aws
python3 write_keypairs_file.py 100
```

The above command generates a `keypairs.py` file with 100 keypairs. You can generate more keypairs than you need, so you can use the same list over and over again, for different numbers of servers. The deployment scripts will only use the first NUM_NODES keypairs.

Step 3

Step 3 is to launch the nodes ("instances") on AWS, to install all the necessary software on them, configure the software, run the software, and more. Here's how you'd do that:

```
# in a Python 2.5-2.7 virtual environment where fabric, boto3, etc. are installed
cd bigchaindb
cd deploy-cluster-aws
./awsdeploy.sh my_deploy_conf.py
# Only if you want to set the replication factor to 3
fab set_replicas:3
# Only if you want to start BigchainDB on all the nodes:
fab start_bigchaindb
```

`awsdeploy.sh` is a Bash script which calls some Python and Fabric scripts. If you're curious what it does, the source code has many explanatory comments.

It should take a few minutes for the deployment to finish. If you run into problems, see the section on **Known Deployment Issues** below.

The EC2 Console has a section where you can see all the instances you have running on EC2. You can `ssh` into a running instance using a command like:

```
ssh -i pem/bigchaindb.pem ubuntu@ec2-52-29-197-211.eu-central-1.compute.amazonaws.com
```

except you'd replace the `ec2-52-29-197-211.eu-central-1.compute.amazonaws.com` with the public DNS name of the instance you want to `ssh` into. You can get that from the EC2 Console: just click on an instance and look in its details pane at the bottom of the screen. Some commands you might try:

```
ip addr show
sudo service rethinkdb status
bigchaindb --help
bigchaindb show-config
```

If you enabled the RethinkDB web interface (by setting `ENABLE_WEB_ADMIN=True` in your AWS configuration file), then you can also check that. The way to do that depends on how `BIND_HTTP_TO_LOCALHOST` was set (in your AWS deployment configuration file):

- If it was set to `False`, then just go to your web browser and visit a web address like `http://ec2-52-29-197-211.eu-central-1.compute.amazonaws.com:8080/`. (Replace `ec2-...aws.com` with the hostname of one of your instances.)
- If it was set to `True` (the default in the example config file), then follow the instructions in the "Via a SOCKS proxy" section of the "Secure your cluster" page of the RethinkDB documentation.

14.10.8 Server Monitoring with New Relic

New Relic is a business that provides several monitoring services. One of those services, called Server Monitoring, can be used to monitor things like CPU usage and Network I/O on BigchainDB instances. To do that:

1. Sign up for a New Relic account
2. Get your New Relic license key
3. Put that key in an environment variable named `NEWRELIC_KEY`. For example, you might add a line like the following to your `~/.bashrc` file (if you use Bash): `export NEWRELIC_KEY=<insert your key here>`
4. Once you've deployed a BigchainDB cluster on AWS as above, you can install a New Relic system monitor (agent) on all the instances using:

```
# in a Python 2.5-2.7 virtual environment where fabric, boto3, etc. are installed
fab install_newrelic
```

Once the New Relic system monitor (agent) is installed on the instances, it will start sending server stats to New Relic on a regular basis. It may take a few minutes for data to show up in your New Relic dashboard (under New Relic Servers).

14.10.9 Shutting Down a Cluster

There are fees associated with running instances on EC2, so if you're not using them, you should terminate them. You can do that using the AWS EC2 Console.

The same is true of your allocated elastic IP addresses. There's a small fee to keep them allocated if they're not associated with a running instance. You can release them using the AWS EC2 Console, or by using a handy little script named `release_eips.py`. For example:

```
$ python release_eips.py
You have 2 allocated elactic IPs which are not associated with instances
0: Releasing 52.58.110.110
(It has Domain = vpc.)
1: Releasing 52.58.107.211
(It has Domain = vpc.)
```

14.10.10 Known Deployment Issues

NetworkError

If you tested with a high sequence it might be possible that you run into an error message like this:

```
NetworkError: Host key for ec2-xx-xx-xx-xx.eu-central-1.compute.amazonaws.com
did not match pre-existing key! Server's key was changed recently, or possible
man-in-the-middle attack.
```

If so, just clean up your `known_hosts` file and start again. For example, you might copy your current `known_hosts` file to `old_known_hosts` like so:

```
mv ~/.ssh/known_hosts ~/.ssh/old_known_hosts
```

Then terminate your instances and try deploying again with a different tag.

Failure of sudo apt-get update

The first thing that's done on all the instances, once they're running, is basically `sudo apt-get update`. Sometimes that fails. If so, just terminate your instances and try deploying again with a different tag. (These problems seem to be time-bounded, so maybe wait a couple of hours before retrying.)

Failure when Installing Base Software

If you get an error with installing the base software on the instances, then just terminate your instances and try deploying again with a different tag.

14.11 Azure Quickstart Template

This page outlines how to run a single BigchainDB node on the Microsoft Azure public cloud, with RethinkDB as the database backend. It uses an Azure Quickstart Template. That template is dated because we now recommend using MongoDB instead of RethinkDB. That's why we moved this page to the Appendices.

Note: There was an Azure quickstart template in the `blockchain` directory of Microsoft's `Azure/azure-quickstart-templates` repository on GitHub. It's gone now; it was replaced by the one described here.

One can deploy a BigchainDB node on Azure using the template in the `bigchaindb-on-ubuntu` directory of Microsoft's `Azure/azure-quickstart-templates` repository on GitHub. Here's how:

1. Go to that directory on GitHub.
2. Click the button labelled **Deploy to Azure**.

3. If you're not already logged in to Microsoft Azure, then you'll be prompted to login. If you don't have an account, then you'll have to create one.
4. Once you are logged in to the Microsoft Azure Portal, you should be taken to a form titled **BigchainDB**. Some notes to help with filling in that form are available below.
5. Deployment takes a few minutes. You can follow the notifications by clicking the bell icon at the top of the screen. At the time of writing, the final deployment operation (running the `init.sh` script) was failing, but a pull request (#2884) has been made to fix that and these instructions say what you can do before that pull request gets merged...
6. Find out the public IP address of the virtual machine in the Azure Portal. Example: `40.69.87.250`
7. ssh in to the virtual machine at that IP address, i.e. do `ssh <Admin_username>@<machine-ip>` where `<Admin_username>` is the admin username you entered into the form and `<machine-ip>` is the virtual machine IP address determined in the last step. Example: `ssh bcdbadmin@40.69.87.250`
8. You should be prompted for a password. Give the `<Admin_password>` you entered into the form.
9. Configure BigchainDB Server by doing:

```
bigchaindb configure rethinkdb
```

It will ask you several questions. You can press `Enter` (or `Return`) to accept the default for all of them *except for one*. When it asks **API Server bind? (default 'localhost:9984'):**, you should answer:

```
API Server bind? (default `localhost:9984`): 0.0.0.0:9984
```

Finally, run BigchainDB Server by doing:

```
bigchaindb start
```

BigchainDB Server should now be running on the Azure virtual machine.

Remember to shut everything down when you're done (via the Azure Portal), because it generally costs money to run stuff on Azure.

14.11.1 Notes on the Blockchain Template Form Fields

BASICS

Resource group - You can use an existing resource group (if you have one) or create a new one named whatever you like, but avoid using fancy characters in the name because Azure might have problems if you do.

Location is the Microsoft Azure data center where you want the BigchainDB node to run. Pick one close to where you are located.

SETTINGS

You can use whatever **Admin_username** and **Admin_password** you like (provided you don't get too fancy). It will complain if your password is too simple. You'll need these later to `ssh` into the virtual machine.

Dns_label_prefix - Once your virtual machine is deployed, it will have a public IP address and a DNS name (hostname) something like `<DNSprefix>.northeurope.cloudapp.azure.com`. The `<DNSprefix>` will be whatever you enter into this field.

Virtual_machine_size - This should be one of Azure's standard virtual machine sizes, such as `Standard_D1_v2`. There's a list of virtual machine sizes in the Azure docs.

_artifacts Location - Leave this alone.

_artifacts Location Sas Token - Leave this alone (blank).

TERMS AND CONDITIONS

Read the terms and conditions. If you agree to them, then check the checkbox.

Finally, click the button labelled **Purchase**. (Generally speaking, it costs money to run stuff on Azure.)

14.12 Generate a Key Pair for SSH

This page describes how to use `ssh-keygen` to generate a public/private RSA key pair that can be used with SSH. (Note: `ssh-keygen` is found on most Linux and Unix-like operating systems; if you're using Windows, then you'll have to use another tool, such as PuTTYgen.)

By convention, SSH key pairs get stored in the `~/.ssh/` directory. Check what keys you already have there:

```
ls -1 ~/.ssh/
```

Next, make up a new key pair name (called `<name>` below). Here are some ideas:

- `aws-bdb-2`
- `tim-bdb-azure`
- `chris-bcdb-key`

Next, generate a public/private RSA key pair with that name:

```
ssh-keygen -t rsa -C "<name>" -f ~/.ssh/<name>
```

It will ask you for a passphrase. You can use whatever passphrase you like, but don't lose it. Two keys (files) will be created in `~/.ssh/`:

1. `~/.ssh/<name>.pub` is the public key
2. `~/.ssh/<name>` is the private key

14.13 Notes for Firewall Setup

This is a page of notes on the ports potentially used by BigchainDB nodes and the traffic they should expect, to help with firewall setup (and security group setup on AWS). This page is *not* a firewall tutorial or step-by-step guide.

14.13.1 Expected Unsolicited Inbound Traffic

Assuming you aren't exposing the RethinkDB web interface on port 8080 (or any other port, because there are more secure ways to access it), there are only three ports that should expect unsolicited inbound traffic:

1. **Port 22** can expect inbound SSH (TCP) traffic from the node administrator (i.e. a small set of IP addresses).
2. **Port 9984** can expect inbound HTTP (TCP) traffic from BigchainDB clients sending transactions to the BigchainDB HTTP API.
3. **Port 9985** can expect inbount WebSocket traffic from BigchainDB clients.

4. If you're using RethinkDB, **Port 29015** can expect inbound TCP traffic from other RethinkDB nodes in the RethinkDB cluster (for RethinkDB intracluster communications).
5. If you're using MongoDB, **Port 27017** can expect inbound TCP traffic from other nodes.

All other ports should only get inbound traffic in response to specific requests from inside the node.

14.13.2 Port 22

Port 22 is the default SSH port (TCP) so you'll at least want to make it possible to SSH in from your remote machine(s).

14.13.3 Port 53

Port 53 is the default DNS port (UDP). It may be used, for example, by some package managers when look up the IP address associated with certain package sources.

14.13.4 Port 80

Port 80 is the default HTTP port (TCP). It's used by some package managers to get packages. It's *not* used by the RethinkDB web interface (see Port 8080 below) or the BigchainDB client-server HTTP API (Port 9984).

14.13.5 Port 123

Port 123 is the default NTP port (UDP). You should be running an NTP daemon on production BigchainDB nodes. NTP daemons must be able to send requests to external NTP servers and accept the respones.

14.13.6 Port 161

Port 161 is the default SNMP port (usually UDP, sometimes TCP). SNMP is used, for example, by some server monitoring systems.

14.13.7 Port 443

Port 443 is the default HTTPS port (TCP). You may need to open it up for outbound requests (and inbound responses) temporarily because some RethinkDB installation instructions use wget over HTTPS to get the RethinkDB GPG key. Package managers might also get some packages using HTTPS.

14.13.8 Port 8080

Port 8080 is the default port used by RethinkDB for its adminstrative web (HTTP) interface (TCP). While you *can*, you shouldn't allow traffic arbitrary external sources. You can still use the RethinkDB web interface by binding it to localhost and then accessing it via a SOCKS proxy or reverse proxy; see "Binding the web interface port" on the RethinkDB page about securing your cluster.

14.13.9 Port 9984

Port 9984 is the default port for the BigchainDB client-server HTTP API (TCP), which is served by Gunicorn HTTP Server. It's *possible* allow port 9984 to accept inbound traffic from anyone, but we recommend against doing that. Instead, set up a reverse proxy server (e.g. using Nginx) and only allow traffic from there. Information about how to do that can be found in the Gunicorn documentation. (They call it a proxy.)

If Gunicorn and the reverse proxy are running on the same server, then you'll have to tell Gunicorn to listen on some port other than 9984 (so that the reverse proxy can listen on port 9984). You can do that by setting `server.bind` to 'localhost:PORT' in the BigchainDB Configuration Settings, where PORT is whatever port you chose (e.g. 9983).

You may want to have Gunicorn and the reverse proxy running on different servers, so that both can listen on port 9984. That would also help isolate the effects of a denial-of-service attack.

14.13.10 Port 9985

Port 9985 is the default port for the BigchainDB WebSocket Event Stream API.

14.13.11 Port 28015

Port 28015 is the default port used by RethinkDB client driver connections (TCP). If your BigchainDB node is just one server, then Port 28015 only needs to listen on localhost, because all the client drivers will be running on localhost. Port 28015 doesn't need to accept inbound traffic from the outside world.

14.13.12 Port 29015

Port 29015 is the default port for RethinkDB intracluster connections (TCP). It should only accept incoming traffic from other RethinkDB servers in the cluster (a list of IP addresses that you should be able to find out).

14.13.13 Other Ports

On Linux, you can use commands such as `netstat -tunlp` or `lsof -i` to get a sense of currently open/listening ports and connections, and the associated processes.

14.14 Notes on NTP Daemon Setup

There are several NTP daemons available, including:

- The reference NTP daemon (`ntpd`) from ntp.org; see their support website
- chrony
- OpenNTPD
- Maybe NTPsec, once it's production-ready
- Maybe Ntimed, once it's production-ready
- More

We suggest you run your NTP daemon in a mode which will tell your OS kernel to handle leap seconds in a particular way: the default NTP way, so that system clock adjustments are localized and not spread out across the minutes, hours, or days surrounding leap seconds (e.g. "slewing" or "smearing"). There's a nice Red Hat Developer Blog post about the various options.

Use the default mode with `ntpd` and `chronyd`. For another NTP daemon, consult its documentation.

It's tricky to make an NTP daemon setup secure. Always install the latest version and read the documentation about how to configure and run it securely. See the notes on firewall setup.

14.14.1 Amazon Linux Instances

If your BigchainDB node is running on an Amazon Linux instance (i.e. a Linux instance packaged by Amazon, not Canonical, Red Hat, or someone else), then an NTP daemon should already be installed and configured. See the EC2 documentation on Setting the Time for Your Linux Instance.

That said, you should check *which* NTP daemon is installed. Is it recent? Is it configured securely?

14.14.2 The Ubuntu ntp Packages

The Ubuntu `ntp` packages are based on the reference implementation of NTP.

The following commands will uninstall the `ntp` and `ntpdate` packages, install the latest `ntp` package (which *might not be based on the latest ntpd code*), and start the NTP daemon (a local NTP server). (`ntpdate` is not reinstalled because it's deprecated and you shouldn't use it.)

```
sudo apt-get --purge remove ntp ntpdate
sudo apt-get autoremove
sudo apt-get update
sudo apt-get install ntp
# That should start the NTP daemon too, but just to be sure:
sudo service ntp restart
```

You can check if `ntpd` is running using `sudo ntpq -p`.

You may want to use different NTP time servers. You can change them by editing the NTP config file `/etc/ntp.conf`.

Note: A server running an NTP daemon can be used by others for DRDoS amplification attacks. The above installation procedure should install a default NTP configuration file `/etc/ntp.conf` with the lines:

```
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery
```

Those lines should prevent the NTP daemon from being used in an attack. (The first line is for IPv4, the second for IPv6.)

There are additional things you can do to make NTP more secure. See the NTP Support Website for more details.

14.15 RethinkDB Requirements

The RethinkDB documentation should be your first source of information about its requirements. This page serves mostly to document some of its more obscure requirements.

RethinkDB Server will run on any modern OS. Note that the Fedora package isn't officially supported. Also, official support for Windows is fairly recent (April 2016).

14.15.1 Storage Requirements

When it comes to storage for RethinkDB, there are many things that are nice to have (e.g. SSDs, high-speed input/output [IOPS], replication, reliability, scalability, pay-for-what-you-use), but there are few *requirements* other than:

1. have enough storage to store all your data (and its replicas), and
2. make sure your storage solution (hardware and interconnects) can handle your expected read & write rates.

For RethinkDB's failover mechanisms to work, every RethinkDB table must have at least three replicas (i.e. a primary replica and two others). For example, if you want to store 10 GB of unique data, then you need at least 30 GB of storage. (Indexes and internal metadata are stored in RAM.)

As for the read & write rates, what do you expect those to be for your situation? It's not enough for the storage system alone to handle those rates: the interconnects between the nodes must also be able to handle them.

Storage Notes Specific to RethinkDB

- The RethinkDB storage engine has a number of SSD optimizations, so you *can* benefit from using SSDs. (source)
- If you have an N-node RethinkDB cluster and 1) you want to use it to store an amount of data D (unique records, before replication), 2) you want the replication factor to be R (all tables), and 3) you want N shards (all tables), then each BigchainDB node must have storage space of at least R×D/N.
- RethinkDB tables can have at most 64 shards. What does that imply? Suppose you only have one table, with 64 shards. How big could that table be? It depends on how much data can be stored in each node. If the maximum amount of data that a node can store is d, then the biggest-possible shard is d, and the biggest-possible table size is 64 times that. (All shard replicas would have to be stored on other nodes beyond the initial 64.) If there are two tables, the second table could also have 64 shards, stored on 64 other maxed-out nodes, so the total amount of unique data in the database would be (64 shards/table)×(2 tables)×d. In general, if you have T tables, the maximum amount of unique data that can be stored in the database (i.e. the amount of data before replication) is 64×T×d.
- When you set up storage for your RethinkDB data, you may have to select a filesystem. (Sometimes, the filesystem is already decided by the choice of storage.) We recommend using a filesystem that supports direct I/O (Input/Output). Many compressed or encrypted file systems don't support direct I/O. The ext4 filesystem supports direct I/O (but be careful: if you enable the data=journal mode, then direct I/O support will be disabled; the default is data=ordered). If your chosen filesystem supports direct I/O and you're using Linux, then you don't need to do anything to request or enable direct I/O. RethinkDB does that.
- RethinkDB stores its data in a specific directory. You can tell RethinkDB *which* directory using the RethinkDB config file, as explained below. In this documentation, we assume the directory is `/data`. If you set up a separate device (partition, RAID array, or logical volume) to store the RethinkDB data, then mount that device on `/data`.

14.15.2 Memory (RAM) Requirements

In their FAQ, RethinkDB recommends that, "RethinkDB servers have at least 2GB of RAM..." (source)

In particular: "RethinkDB requires data structures in RAM on each server proportional to the size of the data on that server's disk, usually around 1% of the size of the total data set." (source) We asked what they meant by "total data set" and they said it's "referring to only the data stored on the particular server."

Also, "The storage engine is used in conjunction with a custom, B-Tree-aware caching engine which allows file sizes many orders of magnitude greater than the amount of available memory. RethinkDB can operate on a terabyte of data with about ten gigabytes of free RAM." (source) (In this case, it's the *cluster* which has a total of one terabyte of data,

and it's the *cluster* which has a total of ten gigabytes of RAM. That is, if you add up the RethinkDB RAM on all the servers, it's ten gigabytes.)

In reponse to our questions about RAM requirements, @danielmewes (of RethinkDB) wrote:

> ... If you replicate the data, the amount of data per server increases accordingly, because multiple copies of the same data will be held by different servers in the cluster.

For example, if you increase the data replication factor from 1 to 2 (i.e. the primary plus one copy), then that will double the RAM needed for metadata. Also from @danielmewes:

> **For reasonable performance, you should probably aim at something closer to 5-10% of the data size.** [Emphasis added] The 1% is the bare minimum and doesn't include any caching. If you want to run near the minimum, you'll also need to manually lower RethinkDB's cache size through the `--cache-size` parameter to free up enough RAM for the metadata overhead...

RethinkDB has documentation about its memory requirements. You can use that page to get a better estimate of how much memory you'll need. In particular, note that RethinkDB automatically configures the cache size limit to be about half the available memory, but it can be no lower than 100 MB. As @danielmewes noted, you can manually change the cache size limit (e.g. to free up RAM for queries, metadata, or other things).

If a RethinkDB process (on a server) runs out of RAM, the operating system will start swapping RAM out to disk, slowing everything down. According to @danielmewes:

> Going into swap is usually pretty bad for RethinkDB, and RethinkDB servers that have gone into swap often become so slow that other nodes in the cluster consider them unavailable and terminate the connection to them. I recommend adjusting RethinkDB's cache size conservatively to avoid this scenario. RethinkDB will still make use of additional RAM through the operating system's block cache (though less efficiently than when it can keep data in its own cache).

14.15.3 Filesystem Requirements

RethinkDB "supports most commonly used file systems" (source) but it has issues with BTRFS (B-tree file system).

It's best to use a filesystem that supports direct I/O, because that will improve RethinkDB performance (if you tell RethinkDB to use direct I/O). Many compressed or encrypted filesystems don't support direct I/O.

14.16 Backing Up and Restoring Data

This page was written when BigchainDB only worked with RethinkDB, so its focus is on RethinkDB-based backup. BigchainDB now supports MongoDB as a backend database and we recommend that you use MongoDB in production. Nevertheless, some of the following backup ideas are still relevant regardless of the backend database being used, so we moved this page to the Appendices.

14.16.1 RethinkDB's Replication as a form of Backup

RethinkDB already has internal replication: every document is stored on *R* different nodes, where *R* is the replication factor (set using `bigchaindb set-replicas R`). Those replicas can be thought of as "live backups" because if one node goes down, the cluster will continue to work and no data will be lost.

At this point, there should be someone saying, "But replication isn't backup¡'

It's true. Replication alone isn't enough, because something bad might happen *inside* the database, and that could affect the replicas. For example, what if someone logged in as a RethinkDB admin and did a "drop table"? We currently plan for each node to be protected by a next-generation firewall (or something similar) to prevent such things from getting very far. For example, see issue #240.

Nevertheless, you should still consider having normal, "cold" backups, because bad things can still happen.

14.16.2 Live Replication of RethinkDB Data Files

Each BigchainDB node stores its subset of the RethinkDB data in one directory. You could set up the node's file system so that directory lives on its own hard drive. Furthermore, you could make that hard drive part of a RAID array, so that a second hard drive would always have a copy of the original. If the original hard drive fails, then the second hard drive could take its place and the node would continue to function. Meanwhile, the original hard drive could be replaced.

That's just one possible way of setting up the file system so as to provide extra reliability.

Another way to get similar reliability would be to mount the RethinkDB data directory on an Amazon EBS volume. Each Amazon EBS volume is, "automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability."

As with shard replication, live file-system replication protects against many failure modes, but it doesn't protect against them all. You should still consider having normal, "cold" backups.

14.16.3 rethinkdb dump (to a File)

RethinkDB can create an archive of all data in the cluster (or all data in specified tables), as a compressed file. According to the RethinkDB blog post when that functionality became available:

> Since the backup process is using client drivers, it automatically takes advantage of the MVCC [multiversion concurrency control] functionality built into RethinkDB. It will use some cluster resources, but will not lock out any of the clients, so you can safely run it on a live cluster.

To back up all the data in a BigchainDB cluster, the RethinkDB admin user must run a command like the following on one of the nodes:

```
rethinkdb dump -e bigchain.bigchain -e bigchain.votes
```

That should write a file named `rethinkdb_dump_<date>_<time>.tar.gz`. The `-e` option is used to specify which tables should be exported. You probably don't need to export the backlog table, but you definitely need to export the bigchain and votes tables. `bigchain.votes` means the `votes` table in the RethinkDB database named `bigchain`. It's possible that your database has a different name: the database name is a BigchainDB configuration setting. The default name is `bigchain`. (Tip: you can see the values of all configuration settings using the `bigchaindb show-config` command.)

There's more information about the `rethinkdb dump` command in the RethinkDB documentation. It also explains how to restore data to a cluster from an archive file.

Notes

- If the `rethinkdb dump` subcommand fails and the last line of the Traceback says "NameError: name 'file' is not defined", then you need to update your RethinkDB Python driver; do a `pip install --upgrade rethinkdb`
- It might take a long time to backup data this way. The more data, the longer it will take.
- You need enough free disk space to store the backup file.
- If a document changes after the backup starts but before it ends, then the changed document may not be in the final backup. This shouldn't be a problem for BigchainDB, because blocks and votes can't change anyway.
- `rethinkdb dump` saves data and secondary indexes, but does *not* save cluster metadata. You will need to recreate your cluster setup yourself after you run `rethinkdb restore`.

- RethinkDB also has subcommands to import/export collections of JSON or CSV files. While one could use those for backup/restore, it wouldn't be very practical.

14.16.4 Client-Side Backup

In the future, it will be possible for clients to query for the blocks containing the transactions they care about, and for the votes on those blocks. They could save a local copy of those blocks and votes.

How could we be sure blocks and votes from a client are valid?

All blocks and votes are signed by cluster nodes (owned and operated by consortium members). Only cluster nodes can produce valid signatures because only cluster nodes have the necessary private keys. A client can't produce a valid signature for a block or vote.

Could we restore an entire BigchainDB database using client-saved blocks and votes?

Yes, in principle, but it would be difficult to know if you've recovered every block and vote. Votes link to the block they're voting on and to the previous block, so one could detect some missing blocks. It would be difficult to know if you've recovered all the votes.

14.16.5 Backup by Copying RethinkDB Data Files

It's *possible* to back up a BigchainDB database by creating a point-in-time copy of the RethinkDB data files (on all nodes, at roughly the same time). It's not a very practical approach to backup: the resulting set of files will be much larger (collectively) than what one would get using `rethinkdb dump`, and there are no guarantees on how consistent that data will be, especially for recently-written data.

If you're curious about what's involved, see the MongoDB documentation about "Backup by Copying Underlying Data Files". (Yes, that's documentation for MongoDB, but the principles are the same.)

See the last subsection of this page for a better way to use this idea.

14.16.6 Incremental or Continuous Backup

Incremental backup is where backup happens on a regular basis (e.g. daily), and each one only records the changes since the last backup.

Continuous backup might mean incremental backup on a very regular basis (e.g. every ten minutes), or it might mean backup of every database operation as it happens. The latter is also called transaction logging or continuous archiving.

At the time of writing, RethinkDB didn't have a built-in incremental or continuous backup capability, but the idea was raised in RethinkDB issues #89 and #5890. On July 5, 2016, Daniel Mewes (of RethinkDB) wrote the following comment on issue #5890: "We would like to add this feature [continuous backup], but haven't started working on it yet."

To get a sense of what continuous backup might look like for RethinkDB, one can look at the continuous backup options available for MongoDB. MongoDB, the company, offers continuous backup with Ops Manager (self-hosted) or Cloud Manager (fully managed). Features include:

- It "continuously maintains backups, so if your MongoDB deployment experiences a failure, the most recent backup is only moments behind..."
- It "offers point-in-time backups of replica sets and cluster-wide snapshots of sharded clusters. You can restore to precisely the moment you need, quickly and safely."
- "You can rebuild entire running clusters, just from your backups."
- It enables, "fast and seamless provisioning of new dev and test environments."

The MongoDB documentation has more details about how Ops Manager Backup works.

Considerations for BigchainDB:

- We'd like the cost of backup to be low. To get a sense of the cost, MongoDB Cloud Manager backup costed $30 / GB / year prepaid. One thousand gigabytes backed up (i.e. about a terabyte) would cost 30 thousand US dollars per year. (That's just for the backup; there's also a cost per server per year.)
- We'd like the backup to be decentralized, with no single point of control or single point of failure. (Note: some file systems have a single point of failure. For example, HDFS has one Namenode.)
- We only care to back up blocks and votes, and once written, those never change. There are no updates or deletes, just new blocks and votes.

14.16.7 Combining RethinkDB Replication with Storage Snapshots

Although it's not advertised as such, RethinkDB's built-in replication feature is similar to continous backup, except the "backup" (i.e. the set of replica shards) is spread across all the nodes. One could take that idea a bit farther by creating a set of backup-only servers with one full backup:

- Give all the original BigchainDB nodes (RethinkDB nodes) the server tag `original`.
- Set up a group of servers running RethinkDB only, and give them the server tag `backup`. The `backup` servers could be geographically separated from all the `original` nodes (or not; it's up to the consortium to decide).
- Clients shouldn't be able to read from or write to servers in the `backup` set.
- Send a RethinkDB reconfigure command to the RethinkDB cluster to make it so that the `original` set has the same number of replicas as before (or maybe one less), and the `backup` set has one replica. Also, make sure the `primary_replica_tag='original'` so that all primary shards live on the `original` nodes.

The RethinkDB documentation on sharding and replication has the details of how to set server tags and do RethinkDB reconfiguration.

Once you've set up a set of backup-only RethinkDB servers, you could make a point-in-time snapshot of their storage devices, as a form of backup.

You might want to disconnect the `backup` set from the `original` set first, and then wait for reads and writes in the `backup` set to stop. (The `backup` set should have only one copy of each shard, so there's no opportunity for inconsistency between shards of the `backup` set.)

You will want to re-connect the `backup` set to the `original` set as soon as possible, so it's able to catch up.

If something bad happens to the entire original BigchainDB cluster (including the `backup` set) and you need to restore it from a snapshot, you can, but before you make BigchainDB live, you should 1) delete all entries in the backlog table, 2) delete all blocks after the last voted-valid block, 3) delete all votes on the blocks deleted in part 2, and 4) rebuild the RethinkDB indexes.

NOTE: Sometimes snapshots are *incremental*. For example, Amazon EBS snapshots are incremental, meaning "only the blocks on the device that have changed after your most recent snapshot are saved. **This minimizes the time required to create the snapshot and saves on storage costs.**" [Emphasis added]

14.17 Licenses

Information about how the BigchainDB Server code and documentation are licensed can be found in the LICENSES.md file of the bigchaindb/bigchaindb repository on GitHub.

14.18 Installing BigchainDB on LXC containers using LXD

Note: This page was contributed by an external contributor and is not actively maintained. We include it in case someone is interested.

You can visit this link to install LXD (instructions here): LXD Install

(assumption is that you are using Ubuntu 14.04 for host/container)

Let us create an LXC container (via LXD) with the following command:

`lxc launch ubuntu:14.04 bigchaindb`

(ubuntu:14.04 - this is the remote server the command fetches the image from) (bigchaindb - is the name of the container)

Below is the `install.sh` script you will need to install BigchainDB within your container.

Here is my `install.sh`:

```
#!/bin/bash
set -ex
export DEBIAN_FRONTEND=noninteractive
apt-get install -y wget
source /etc/lsb-release && echo "deb http://download.rethinkdb.com/apt $DISTRIB_
↪CODENAME main" | sudo tee /etc/apt/sources.list.d/rethinkdb.list
wget -qO- https://download.rethinkdb.com/apt/pubkey.gpg | sudo apt-key add -
apt-get update
apt-get install -y rethinkdb python3-pip
pip3 install --upgrade pip wheel setuptools
pip install ptpython bigchaindb
```

Copy/Paste the above `install.sh` into the directory/path you are going to execute your LXD commands from (ie. the host).

Make sure your container is running by typing:

`lxc list`

Now, from the host (and the correct directory) where you saved `install.sh`, run this command:

`cat install.sh | lxc exec bigchaindb /bin/bash`

If you followed the commands correctly, you will have successfully created an LXC container (using LXD) that can get you up and running with BigchainDB in <5 minutes (depending on how long it takes to download all the packages).

14.19 The Transaction Schema Files

BigchainDB checks all *transactions* (JSON documents) against a formal schema defined in some JSON Schema files named transaction.yaml, transaction_create.yaml and transaction_transfer.yaml. The contents of those files are copied below. To understand those contents (i.e. JSON Schema), check out "Understanding JSON Schema" by Michael Droettboom or json-schema.org.

14.19.1 transaction.yaml

```
---
"$schema": "http://json-schema.org/draft-04/schema#"
id: "http://www.bigchaindb.com/schema/transaction.json"
type: object
additionalProperties: false
title: Transaction Schema
required:
- id
- inputs
- outputs
- operation
- metadata
- asset
- version
properties:
  id:
    "$ref": "#/definitions/sha3_hexdigest"
  operation:
    "$ref": "#/definitions/operation"
  asset:
    "$ref": "#/definitions/asset"
  inputs:
    type: array
    title: "Transaction inputs"
    items:
      "$ref": "#/definitions/input"
  outputs:
    type: array
    items:
      "$ref": "#/definitions/output"
  metadata:
    "$ref": "#/definitions/metadata"
  version:
    type: string
    pattern: "^1\\.0$"
definitions:
  offset:
    type: integer
    minimum: 0
  base58:
    pattern: "[1-9a-zA-Z^OIl]{43,44}"
    type: string
  public_keys:
    anyOf:
    - type: array
      items:
        "$ref": "#/definitions/base58"
    - type: 'null'
  sha3_hexdigest:
    pattern: "[0-9a-f]{64}"
    type: string
  uuid4:
    pattern: "[a-f0-9]{8}-[a-f0-9]{4}-4[a-f0-9]{3}-[89ab][a-f0-9]{3}-[a-f0-9]{12}"
    type: string
  operation:
    type: string
    enum:
    - CREATE
```

```
    - TRANSFER
    - GENESIS
  asset:
    type: object
    additionalProperties: false
    properties:
      id:
        "$ref": "#/definitions/sha3_hexdigest"
      data:
        anyOf:
        - type: object
          additionalProperties: true
        - type: 'null'
  output:
    type: object
    additionalProperties: false
    required:
    - amount
    - condition
    - public_keys
    properties:
      amount:
        type: string
        pattern: "^[0-9]{1,20}$"
      condition:
        type: object
        additionalProperties: false
        required:
        - details
        - uri
        properties:
          details:
            "$ref": "#/definitions/condition_details"
          uri:
            type: string
            pattern: "^ni:///sha-256;([a-zA-Z0-9_-]{0,86})[?]\
              (fpt=(ed25519|threshold)-sha-256(&)?|cost=[0-9]+(&)?|\
              subtypes=ed25519-sha-256(&)?){2,3}$"
      public_keys:
        "$ref": "#/definitions/public_keys"
  input:
    type: "object"
    additionalProperties: false
    required:
    - owners_before
    - fulfillment
    properties:
      owners_before:
        "$ref": "#/definitions/public_keys"
      fulfillment:
        anyOf:
        - type: string
          pattern: "^[a-zA-Z0-9_-]*$"
        - "$ref": "#/definitions/condition_details"
      fulfills:
        anyOf:
        - type: 'object'
          additionalProperties: false
```

```
          required:
          - output_index
          - transaction_id
          properties:
            output_index:
              "$ref": "#/definitions/offset"
            transaction_id:
              "$ref": "#/definitions/sha3_hexdigest"
        - type: 'null'
  metadata:
    anyOf:
    - type: object
      additionalProperties: true
      minProperties: 1
    - type: 'null'
  condition_details:
    anyOf:
    - type: object
      additionalProperties: false
      required:
      - type
      - public_key
      properties:
        type:
          type: string
          pattern: "^ed25519-sha-256$"
        public_key:
          "$ref": "#/definitions/base58"
    - type: object
      additionalProperties: false
      required:
      - type
      - threshold
      - subconditions
      properties:
        type:
          type: "string"
          pattern: "^threshold-sha-256$"
        threshold:
          type: integer
          minimum: 1
          maximum: 100
        subconditions:
          type: array
          items:
            "$ref": "#/definitions/condition_details"
```

14.19.2 transaction_create.yaml

```
---
"$schema": "http://json-schema.org/draft-04/schema#"
type: object
title: Transaction Schema - CREATE/GENESIS specific constraints
required:
- asset
- inputs
```

```
properties:
  asset:
    additionalProperties: false
    properties:
      data:
        anyOf:
        - type: object
          additionalProperties: true
        - type: 'null'
    required:
    - data
  inputs:
    type: array
    title: "Transaction inputs"
    maxItems: 1
    minItems: 1
    items:
      type: "object"
      required:
      - fulfills
      properties:
        fulfills:
            type: "null"
```

14.19.3 transaction_transfer.yaml

```
---
"$schema": "http://json-schema.org/draft-04/schema#"
type: object
title: Transaction Schema - TRANSFER specific properties
required:
- asset
properties:
  asset:
    additionalProperties: false
    properties:
      id:
        "$ref": "#/definitions/sha3_hexdigest"
    required:
    - id
  inputs:
    type: array
    title: "Transaction inputs"
    minItems: 1
    items:
      type: "object"
      required:
      - fulfills
      properties:
        fulfills:
            type: "object"
definitions:
  sha3_hexdigest:
    pattern: "[0-9a-f]{64}"
    type: string
```

14.20 The Vote Schema File

BigchainDB checks all *votes* (JSON documents) against a formal schema defined in a JSON Schema file named vote.yaml. The contents of that file are copied below. To understand those contents (i.e. JSON Schema), check out "Understanding JSON Schema" by Michael Droettboom or json-schema.org.

14.20.1 vote.yaml

```
---
"$schema": "http://json-schema.org/draft-04/schema#"
id: "http://www.bigchaindb.com/schema/vote.json"
type: object
additionalProperties: false
title: Vote Schema
required:
- node_pubkey
- signature
- vote
properties:
  node_pubkey:
    type: "string"
    pattern: "[1-9a-zA-Z^OIl]{43,44}"
  signature:
    type: "string"
    pattern: "[1-9a-zA-Z^OIl]{86,88}"
  vote:
    type: "object"
    additionalProperties: false
    required:
    - invalid_reason
    - is_block_valid
    - previous_block
    - voting_for_block
    - timestamp
    properties:
      previous_block:
        "$ref": "#/definitions/sha3_hexdigest"
      voting_for_block:
        "$ref": "#/definitions/sha3_hexdigest"
      is_block_valid:
        type: "boolean"
      invalid_reason:
        anyOf:
        - type: "string"
        - type: "null"
      timestamp:
        type: "string"
        pattern: "[0-9]{10}"
definitions:
  sha3_hexdigest:
    pattern: "[0-9a-f]{64}"
    type: string
```

Python Module Index

b

bigchaindb.backend, 140
bigchaindb.backend.admin, 147
bigchaindb.backend.changefeed, 141
bigchaindb.backend.connection, 140
bigchaindb.backend.query, 142
bigchaindb.backend.rethinkdb, 147
bigchaindb.backend.rethinkdb.admin, 148
bigchaindb.backend.rethinkdb.changefeed, 148
bigchaindb.backend.rethinkdb.connection, 147
bigchaindb.backend.rethinkdb.query, 148
bigchaindb.backend.rethinkdb.schema, 148
bigchaindb.backend.schema, 146
bigchaindb.backend.utils, 147
bigchaindb.commands, 150
bigchaindb.commands.bigchaindb, 150
bigchaindb.commands.utils, 150
bigchaindb.pipelines.block, 137
bigchaindb.pipelines.election, 139
bigchaindb.pipelines.stale, 139
bigchaindb.pipelines.vote, 138

HTTP Routing Table

/api

GET /api/v1/assets, 99
GET /api/v1/assets?search={text_search},
99
GET /api/v1/assets?search={text_search}&limit={n_documents},
100
GET /api/v1/blocks, 104
GET /api/v1/blocks/{block_id}, 103
GET /api/v1/blocks?transaction_id={transaction_id}&status={UNDECIDED|VALID|INVALID},
105
GET /api/v1/metadata, 101
GET /api/v1/metadata/?search={text_search},
101
GET /api/v1/metadata/?search={text_search}&limit={n_documents},
102
GET /api/v1/outputs, 96
GET /api/v1/outputs?public_key={public_key},
96
GET /api/v1/outputs?public_key={public_key}&spent=false,
97
GET /api/v1/outputs?public_key={public_key}&spent=true,
97
GET /api/v1/statuses, 98
GET /api/v1/statuses?block_id={block_id},
99
GET /api/v1/statuses?transaction_id={transaction_id},
98
GET /api/v1/transactions, 91
GET /api/v1/transactions/{transaction_id},
90
GET /api/v1/transactions?asset_id={asset_id}&operation={CREATE|TRANSFER},
92
GET /api/v1/votes?block_id={block_id},
106
POST /api/v1/transactions, 94

Index

Symbols

__init__() (bigchaindb.backend.connection.Connection method), 140
__init__() (bigchaindb.core.Bigchain method), 132

A

associative array, **127**

B

Bigchain (class in bigchaindb), 132
bigchaindb.backend (module), 140
bigchaindb.backend.admin (module), 147
bigchaindb.backend.changefeed (module), 141
bigchaindb.backend.connection (module), 140
bigchaindb.backend.query (module), 142
bigchaindb.backend.rethinkdb (module), 147
bigchaindb.backend.rethinkdb.admin (module), 148
bigchaindb.backend.rethinkdb.changefeed (module), 148
bigchaindb.backend.rethinkdb.connection (module), 147
bigchaindb.backend.rethinkdb.query (module), 148
bigchaindb.backend.rethinkdb.schema (module), 148
bigchaindb.backend.schema (module), 146
bigchaindb.backend.utils (module), 147
bigchaindb.commands (module), 150
bigchaindb.commands.bigchaindb (module), 150
bigchaindb.commands.utils (module), 150
bigchaindb.pipelines.block (module), 137
bigchaindb.pipelines.election (module), 139
bigchaindb.pipelines.stale (module), 139
bigchaindb.pipelines.vote (module), 138
block_election_status() (bigchaindb.Bigchain method), 136
BLOCK_INVALID (bigchaindb.Bigchain attribute), 132
BLOCK_UNDECIDED (bigchaindb.Bigchain attribute), 132
BLOCK_VALID (bigchaindb.Bigchain attribute), 132
BlockPipeline (class in bigchaindb.pipelines.block), 137

C

ChangeFeed (class in bigchaindb.backend.changefeed), 141
check_for_quorum() (bigchaindb.pipelines.election.Election method), 139
check_transactions() (bigchaindb.pipelines.stale.StaleTransactionMonitor method), 139
configure_bigchaindb() (in module bigchaindb.commands.utils), 150
connect() (bigchaindb.backend.connection.Connection method), 141
connect() (in module bigchaindb.backend.connection), 140
Connection (class in bigchaindb.backend.connection), 140
count_backlog() (in module bigchaindb.backend.query), 145
count_blocks() (in module bigchaindb.backend.query), 145
create() (bigchaindb.pipelines.block.BlockPipeline method), 137
create_block() (bigchaindb.Bigchain method), 135
create_database() (in module bigchaindb.backend.schema), 146
create_genesis_block() (bigchaindb.Bigchain method), 135
create_indexes() (in module bigchaindb.backend.schema), 146
create_pipeline() (in module bigchaindb.pipelines.block), 138
create_pipeline() (in module bigchaindb.pipelines.stale), 139
create_pipeline() (in module bigchaindb.pipelines.vote), 139
create_tables() (in module bigchaindb.backend.schema), 146

D

delete_transaction() (bigchaindb.Bigchain method), 133

delete_transaction() (in module bigchaindb.backend.query), 142
delete_tx() (bigchaindb.pipelines.block.BlockPipeline method), 137
drop_database() (in module bigchaindb.backend.schema), 146

E

Election (class in bigchaindb.pipelines.election), 139

F

federation (bigchaindb.Bigchain attribute), 132
filter_tx() (bigchaindb.pipelines.block.BlockPipeline method), 137

G

get_asset_by_id() (bigchaindb.Bigchain method), 134
get_asset_by_id() (in module bigchaindb.backend.query), 143
get_assets() (bigchaindb.Bigchain method), 136
get_assets() (in module bigchaindb.backend.query), 144
get_block() (bigchaindb.Bigchain method), 133
get_block() (in module bigchaindb.backend.query), 144
get_blocks_status_containing_tx() (bigchaindb.Bigchain method), 134
get_blocks_status_from_transaction() (in module bigchaindb.backend.query), 143
get_changefeed() (in module bigchaindb.backend.changefeed), 141
get_changefeed() (in module bigchaindb.backend.rethinkdb.changefeed), 148
get_changefeed() (in module bigchaindb.pipelines.vote), 139
get_config() (in module bigchaindb.backend.rethinkdb.admin), 148
get_genesis_block() (in module bigchaindb.backend.query), 145
get_last_voted_block() (bigchaindb.Bigchain method), 136
get_last_voted_block_id() (in module bigchaindb.backend.query), 145
get_metadata() (bigchaindb.Bigchain method), 136
get_metadata() (in module bigchaindb.backend.query), 144
get_new_blocks_feed() (in module bigchaindb.backend.query), 145
get_outputs_filtered() (bigchaindb.Bigchain method), 135
get_owned_ids() (bigchaindb.Bigchain method), 134
get_owned_ids() (in module bigchaindb.backend.query), 143
get_spending_transactions() (in module bigchaindb.backend.query), 143
get_spent() (bigchaindb.Bigchain method), 134
get_spent() (in module bigchaindb.backend.query), 143
get_stale_transactions() (bigchaindb.Bigchain method), 133
get_stale_transactions() (in module bigchaindb.backend.query), 142
get_status() (bigchaindb.Bigchain method), 134
get_transaction() (bigchaindb.Bigchain method), 133
get_transaction_from_backlog() (in module bigchaindb.backend.query), 142
get_transaction_from_block() (in module bigchaindb.backend.query), 142
get_transactions_filtered() (bigchaindb.Bigchain method), 135
get_txids_filtered() (in module bigchaindb.backend.query), 145
get_votes_by_block_id() (in module bigchaindb.backend.query), 143
get_votes_by_block_id_and_voter() (in module bigchaindb.backend.query), 143
get_votes_for_blocks_by_voter() (in module bigchaindb.backend.query), 144

H

has_previous_vote() (bigchaindb.Bigchain method), 135

I

init_database() (in module bigchaindb.backend.schema), 146
input_on_stderr() (in module bigchaindb.commands.utils), 151
is_new_transaction() (bigchaindb.Bigchain method), 133

M

ModuleDispatchRegistrationError, 147
mongodb_host() (in module bigchaindb.commands.utils), 151

P

prepare_genesis_block() (bigchaindb.Bigchain method), 135

R

reassign_transaction() (bigchaindb.Bigchain method), 133
reassign_transactions() (bigchaindb.pipelines.stale.StaleTransactionMonitor method), 139
reconfigure() (in module bigchaindb.backend.rethinkdb.admin), 148
requeue_transactions() (bigchaindb.pipelines.election.Election method), 139
RethinkDBChangeFeed (class in bigchaindb.backend.rethinkdb.changefeed), 148

RethinkDBConnection (class in bigchaindb.backend.rethinkdb.connection), 147
run() (bigchaindb.backend.connection.Connection method), 141
run() (bigchaindb.backend.rethinkdb.connection.RethinkDBConnection method), 147
run_changefeed() (bigchaindb.backend.changefeed.ChangeFeed method), 141
run_changefeed() (in module bigchaindb.backend.rethinkdb.changefeed), 148
run_configure() (in module bigchaindb.commands.bigchaindb), 150
run_drop() (in module bigchaindb.commands.bigchaindb), 150
run_export_my_pubkey() (in module bigchaindb.commands.bigchaindb), 150
run_forever() (bigchaindb.backend.changefeed.ChangeFeed method), 141
run_init() (in module bigchaindb.commands.bigchaindb), 150
run_show_config() (in module bigchaindb.commands.bigchaindb), 150
run_start() (in module bigchaindb.commands.bigchaindb), 150

S

set_replicas() (in module bigchaindb.backend.rethinkdb.admin), 149
set_shards() (in module bigchaindb.backend.rethinkdb.admin), 149
StaleTransactionMonitor (class in bigchaindb.pipelines.stale), 139
start() (in module bigchaindb.commands.utils), 151
start() (in module bigchaindb.pipelines.block), 138
start() (in module bigchaindb.pipelines.stale), 139
start() (in module bigchaindb.pipelines.vote), 139
start_logging_process() (in module bigchaindb.commands.utils), 150
start_rethinkdb() (in module bigchaindb.commands.utils), 151

T

TABLES (in module bigchaindb.backend.schema), 146
text_search() (bigchaindb.Bigchain method), 136
text_search() (in module bigchaindb.backend.query), 145
tx_collector() (in module bigchaindb.pipelines.block), 138
TX_IN_BACKLOG (bigchaindb.Bigchain attribute), 132
TX_UNDECIDED (bigchaindb.Bigchain attribute), 132
TX_VALID (bigchaindb.Bigchain attribute), 132

U

ungroup() (bigchaindb.pipelines.vote.Vote method), 138
unwind_block_transactions() (in module bigchaindb.backend.rethinkdb.query), 148
update_transaction() (in module bigchaindb.backend.query), 142

V

validate_block() (bigchaindb.Bigchain method), 135
validate_language() (in module bigchaindb.backend.schema), 147
validate_language_key() (in module bigchaindb.backend.schema), 146
validate_transaction() (bigchaindb.Bigchain method), 133
validate_tx() (bigchaindb.pipelines.block.BlockPipeline method), 137
validate_tx() (bigchaindb.pipelines.vote.Vote method), 138
Vote (class in bigchaindb.pipelines.vote), 138
vote() (bigchaindb.Bigchain method), 136
vote() (bigchaindb.pipelines.vote.Vote method), 138

W

write() (bigchaindb.pipelines.block.BlockPipeline method), 137
write_assets() (bigchaindb.Bigchain method), 136
write_assets() (in module bigchaindb.backend.query), 144
write_block() (bigchaindb.Bigchain method), 135
write_block() (in module bigchaindb.backend.query), 144
write_metadata() (bigchaindb.Bigchain method), 136
write_metadata() (in module bigchaindb.backend.query), 144
write_transaction() (bigchaindb.Bigchain method), 132
write_transaction() (in module bigchaindb.backend.query), 142
write_vote() (bigchaindb.Bigchain method), 136
write_vote() (bigchaindb.pipelines.vote.Vote method), 139
write_vote() (in module bigchaindb.backend.query), 145