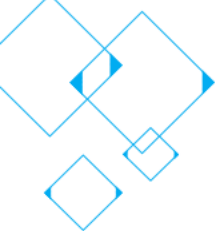


第3章 FISCO BCOS区块链搭建（下）



重航区块链竞赛组

CONTENTS

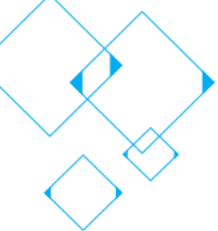
目录

第一章 星型拓扑网络节点搭建

第二章 并行多组网络节点搭建

第三章 国密版FISCO BCOS搭建





CONTENTS

章节

第一章 星型拓扑网络节点搭建

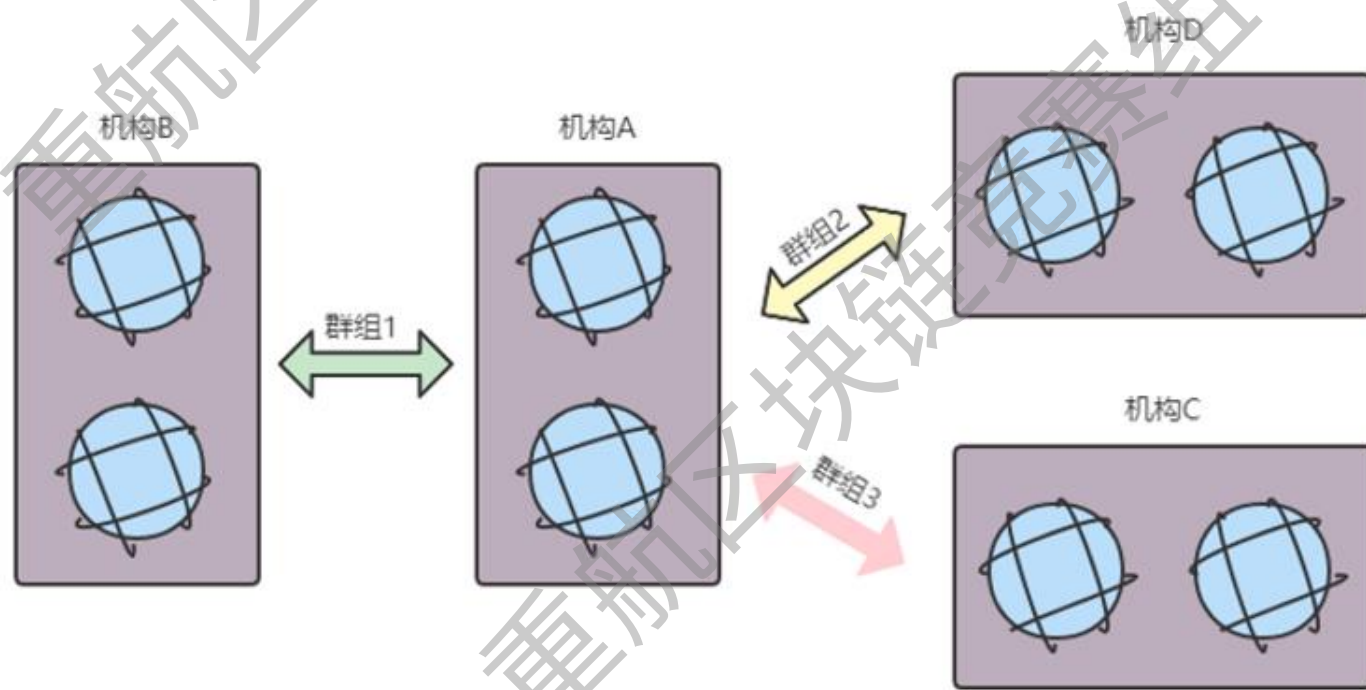
1.1 搭建星型拓扑FISCO BCSO区块链



搭建星型拓扑FISCO BCSO区块链

● 场景描述

- 星型拓扑结构是区块链中常用的组网方式，区块链中运行多个机构节点，中心机构节点同属于多个群组，其他每家机构属于不同的群组。本节将使用开发部署工具搭建一个单机、4机构、3群组、8节点的 FISCO BCOS 联盟链，组网结构如图。



搭建星型拓扑FISCO BCSO区块链

● 组网描述

- agencyA: 在127.0.0.1上有2个节点，同时属于group1、group2和group3;
- agencyB: 在127.0.0.1上有2个节点，同时属于group1;
- agencyC: 在127.0.0.1上有2个节点，同时属于group2;
- agencyD: 在127.0.0.1上有2个节点，同时属于group3;

搭建星型拓扑FISCO BCSO区块链

- 生成组网配置文件ipconf

- 命令: `cat > ipconf << EOF`
- 随后依次输入如下内容, **注意参数之间的空格, 不能有空行**, 输入完成后回车退出。
 - ✓ `127.0.0.1:2 agencyA 1, 2, 3`
 - ✓ `127.0.0.1:2 agencyB 1`
 - ✓ `127.0.0.1:2 agencyC 2`
 - ✓ `127.0.0.1:2 agencyD 3`
 - ✓ `EOF`

```
$ cat > ipconf << EOF
> 127.0.0.1:2 agencyA 1,2,3
> 127.0.0.1:2 agencyB 1
> 127.0.0.1:2 agencyC 2
> 127.0.0.1:2 agencyD 3
> EOF
```

搭建星型拓扑FISCO BCSO区块链

- 组网配置文件内容的格式：IP:NUM AgencyName GroupList
 - **IP:NUM**: 表示机器的IP地址以及该机器上的节点数。
 - **AgencyName**: 表示机构名，用于指定使用的机构证书。
 - **GroupList**: 表示该行生成的节点所属的组，若有多个群组，以`,`分割。
- 示例
 - 127.0.0.1:2 agencyA 1, 2, 3
 - 上述示例表示在本机构建2个节点，机构为agencyA，所属的群组为群组1、群组2和群组3。

搭建星型拓扑FISCO BCSO区块链

● 构建星型拓扑网络节点

➤ 命令: `bash build_chain.sh -f ipconf -p 30300,20200,8545`

```
$ bash build_chain.sh -f ipconf -p 30300,20200,8545
##### 100.0%
=====
Generating CA key...
=====
...
=====
Group:1 has 4 nodes
Group:2 has 4 nodes
Group:3 has 4 nodes
=====
[INFO] IP List File   : star_ipconf
[INFO] Start Port    : 30300 20200 8545
[INFO] Server IP     : 127.0.0.1:2 127.0.0.1:2 127.0.0.1:2 127.0.0.1:2
[INFO] Output Dir    : /root/test/nodes
[INFO] CA Path       : /root/test/nodes/cert/
=====
[INFO] Execute the download_console.sh script in directory named by IP to get FISCO-BCOS console.
e.g.  bash /root/test/nodes/127.0.0.1/download_console.sh -f
=====
[INFO] All completed. Files in /root/test/nodes
```


搭建星型拓扑FISCO BCSO区块链

- 启动节点

➤ 命令: `bash nodes/127.0.0.1/start_all.sh`

```
$ bash nodes/127.0.0.1/start_all.sh
```

```
try to start node0  
try to start node1  
try to start node2  
try to start node3  
try to start node4  
try to start node5  
try to start node6  
try to start node7
```

```
node0 start successfully  
node1 start successfully  
node2 start successfully  
node7 start successfully  
node4 start successfully  
node5 start successfully  
node3 start successfully  
node6 start successfully
```

所有节点均启动成功

搭建星型拓扑FISCO BCSO区块链

● 检查节点进程

- 进程查询命令：`ps -ef | grep -v grep | grep fisco-bcos`
- 正常情况下可以看到有8个进程，如果不为8，请检查端口是否占用。

```
$ ps -ef | grep -v grep | grep fisco-bcos
```

root	46984	1	4	17:03	pts/2	00:00:12	/root/test/nodes/127.0.0.1/node0/../../fisco-bcos -c config.ini
root	46986	1	1	17:03	pts/2	00:00:04	/root/test/nodes/127.0.0.1/node7/../../fisco-bcos -c config.ini
root	46988	1	1	17:03	pts/2	00:00:04	/root/test/nodes/127.0.0.1/node2/../../fisco-bcos -c config.ini
root	46990	1	1	17:03	pts/2	00:00:04	/root/test/nodes/127.0.0.1/node4/../../fisco-bcos -c config.ini
root	46992	1	1	17:03	pts/2	00:00:04	/root/test/nodes/127.0.0.1/node3/../../fisco-bcos -c config.ini
root	46997	1	1	17:03	pts/2	00:00:04	/root/test/nodes/127.0.0.1/node5/../../fisco-bcos -c config.ini
root	46999	1	4	17:03	pts/2	00:00:12	/root/test/nodes/127.0.0.1/node1/../../fisco-bcos -c config.ini
root	47002	1	1	17:03	pts/2	00:00:04	/root/test/nodes/127.0.0.1/node6/../../fisco-bcos -c config.ini

节点的进程ID

搭建星型拓扑FISCO BCSO区块链

● 检查agencyA的节点共识

- node0和node1是机构agencyA的节点，在群组1、群组2和群组3中都有参与共识。
- 查看node0共识状态: `tail -f nodes/127.0.0.1/node0/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node0/log/log* | grep +++
```

node0在群组1、群组2和群组3中都有共识

```
info|2022-04-22 09:32:39.326476|[g:3][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=1
info|2022-04-22 09:32:39.327800|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=1
info|2022-04-22 09:32:42.362989|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=1
```

- 查看node1共识状态: `tail -f nodes/127.0.0.1/node1/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node1/log/log* | grep +++
```

node1在群组1、群组2和群组3中都有共识

```
info|2022-04-22 09:29:18.363877|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=1
info|2022-04-22 09:29:18.384122|[g:3][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=1
info|2022-04-22 09:29:18.539780|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=1
```

搭建星型拓扑FISCO BCSO区块链

● 检查agencyB的节点共识

➤ node2和node3是机构agencyB的节点，只在群组1中参与共识。

➤ 查看node2共识状态: `tail -f nodes/127.0.0.1/node2/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node2/log/log* | grep +++
info|2022-04-22 09:31:00.483973|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=
info|2022-04-22 09:31:04.517980|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=
info|2022-04-22 09:31:08.561123|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=
```

node2只在群组1中有共识

➤ 查看node3共识状态: `tail -f nodes/127.0.0.1/node3/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node3/log/log* | grep +++
info|2022-04-22 09:31:50.864260|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=
info|2022-04-22 09:31:54.925178|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=
info|2022-04-22 09:31:58.962314|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=
```

node3只在群组1中有共识

搭建星型拓扑FISCO BCSO区块链

● 检查agencyC的节点共识

➤ node4和node5是机构agencyC的节点，只在群组2中参与共识。

➤ 查看node4共识状态: `tail -f nodes/127.0.0.1/node4/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node4/log/log* | grep +++
```

node4只在群组2中有共识

```
info|2022-04-22 09:42:55.518588|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:42:59.559012|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:43:03.591684|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

➤ 查看node5共识状态: `tail -f nodes/127.0.0.1/node5/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node5/log/log* | grep +++
```

node5只在群组2中有共识

```
info|2022-04-22 09:43:08.640232|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:43:12.695242|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:43:16.727715|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

搭建星型拓扑FISCO BCSO区块链

● 检查agencyD的节点共识

➤ node6和node7是机构agencyD的节点，只在群组3中参与共识。

➤ 查看node6共识状态: `tail -f nodes/127.0.0.1/node6/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node6/log/log* | grep +++
```

node6只在群组3中有共识

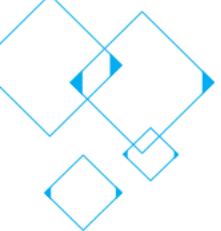
```
info|2022-04-22 09:43:19.737656|[g:3][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:43:23.773861|[g:3][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:43:27.809210|[g:3][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

➤ 查看node7共识状态: `tail -f nodes/127.0.0.1/node7/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node7/log/log* | grep +++
```

node7只在群组3中有共识

```
info|2022-04-22 09:43:28.817299|[g:3][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:43:32.853052|[g:3][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:43:36.930140|[g:3][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

CONTENTS

章节

第二章 并行多组网络节点搭建

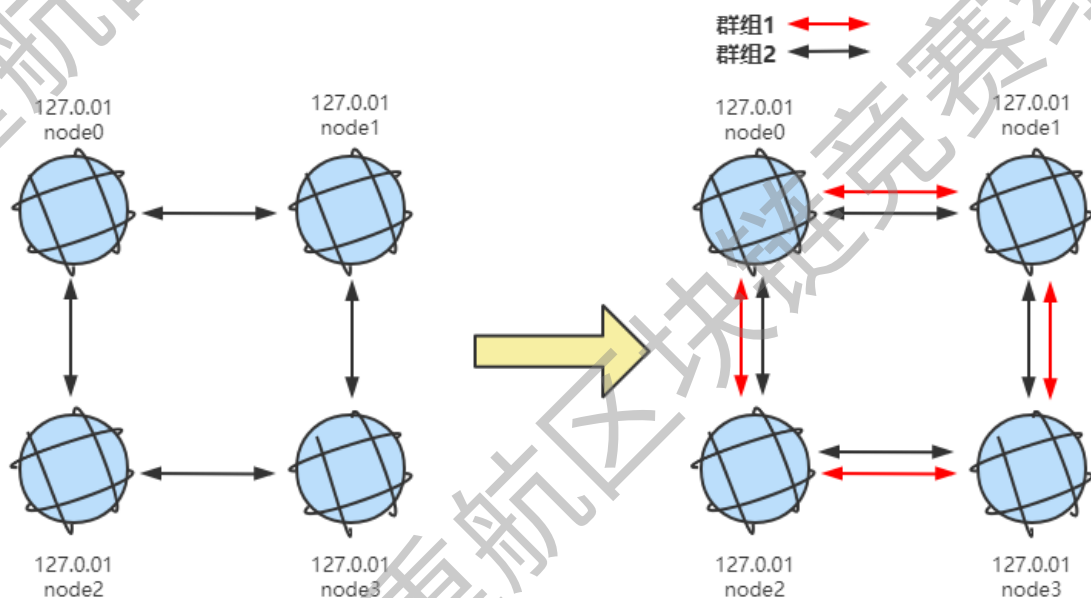
2.1 搭建并行多组FISCO BCOS区块链



搭建并行多组FISCO BCOS区块链

● 场景描述

- 本节将使用开发部署工具搭建一个**单机、2群组、4节点**的 FISCO BCOS 联盟链，为演示并行多组的扩容流程，将先构建单群组四节点网络，随后将群组2加入到区块链中组网结构，如图所示。



搭建并行多组FISCO BCOS区块链

- 构建单群组网络节点

- 命令: `bash build_chain.sh -l 127.0.0.1:4 -o multi_nodes -p 30300,20200,8545`

```
$ bash build_chain.sh -l 127.0.0.1:4 -o multi_nodes -p 30300,20200,8545
##### 100.0%
=====
Generating CA key...
=====
...
=====
[INFO] Start Port      : 20000 20100 7545
[INFO] Server IP       : 127.0.0.1:4
[INFO] Output Dir       : /root/test/multi_nodes
[INFO] CA Path          : /root/test/multi_nodes/cert/
=====
[INFO] Execute the download_console.sh script in directory named by IP to get FISCO-BCOS console.
e.g. bash /root/test/multi_nodes/127.0.0.1/download_console.sh -f
=====
[INFO] All completed. Files in /root/test/multi_nodes
```

构建成功

搭建并行多组FISCO BCOS区块链

- 启动所有节点

➤ 命令: `bash multi_nodes/127.0.0.1/start_all.sh`

```
$ bash multi_nodes/127.0.0.1/start_all.sh
```

```
try to start node0
```

```
try to start node1
```

```
try to start node2
```

```
try to start node3
```

```
node2 start successfully
```

```
node0 start successfully
```

```
node1 start successfully
```

```
node3 start successfully
```

节点启动成功

搭建并行多组FISCO BCOS区块链

● 检查节点共识

- 查看node0共识: `tail -f multi_nodes/127.0.0.1/node0/log/log* | grep +++`

```
$ tail -f multi_nodes/127.0.0.1/node0/log/* | grep +++
info|2021-12-29 17:38:43.167405|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2021-12-29 17:38:50.261906|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2021-12-29 17:14:14.880485|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

此时只在群组1中有共识

- 查看node1共识: `tail -f multi_nodes/127.0.0.1/node1/log/log* | grep +++`

```
$ tail -f multi_nodes/127.0.0.1/node1/log/* | grep +++
info|2022-04-27 03:59:59.217397|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
info|2022-04-27 04:59:57.152141|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
info|2022-04-27 05:59:59.364964|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
```

此时只在群组1中有共识

搭建并行多组FISCO BCOS区块链

● 检查节点共识

➤ 查看node2共识: `tail -f multi_nodes/127.0.0.1/node2/log/log* | grep +++`

```
$ tail -f multi_nodes/127.0.0.1/node2/log/* | grep +++
info|2022-04-27 00:59:57.187483|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
info|2022-04-27 01:59:59.095090|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
info|2022-04-27 02:59:57.067753|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
```

此时只在群组1中有共识

➤ 查看node3共识: `tail -f multi_nodes/127.0.0.1/node3/log/log* | grep +++`

```
$ tail -f multi_nodes/127.0.0.1/node3/log/* | grep +++
info|2022-04-26 19:59:57.850030|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
info|2022-04-26 21:59:58.439482|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
info|2022-04-26 23:59:58.869965|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
```

此时只在群组1中有共识

搭建并行多组FISCO BCOS区块链

- 扩容群组（将群组2添加到区块链）

- 由于在并行多组区块链中，每个群组的 ini 文件文件相同，但 genesis 文件中的 [group.id] 不同，为群组号，所以我们需要拷贝群组1的配置文件（genesis 和 ini 文件），并修改 genesis 文件中的群组号。
- 为减少路径输入引起的麻烦和错误，我们先进入节点目录
 - ✓ `cd multi_nodes/127.0.0.1`
- 然后拷贝节点 node0 中的群组1的配置文件 group.1.ini ，并将其命名为 group.2.ini
 - ✓ `cp node0/conf/group.1.ini node0/conf/group.2.ini`

搭建并行多组FISCO BCOS区块链

- 接着拷贝节点node0中的群组1的配置文件group.1.genesis，并将其命名为group.2.genesis
 - ✓ `cp node0/conf/group.1.genesis node0/conf/group.2.genesis`
- 验证是否拷贝成功，出现group.2.ini和group.2.genesis文件即拷贝成功
 - ✓ `ls node0/conf`

```
$ cd multi_nodes/127.0.0.1
$ cp node0/conf/group.1.ini node0/conf/group.2.ini
$ cp node0/conf/group.1.genesis node0/conf/group.2.genesis
$ ls node0/conf
ca.crt  group.1.genesis  group.1.ini  group.2.genesis  group.2.ini  node.crt  node.key  node.nodeid
```

搭建并行多组FISCO BCOS区块链

- 修改 group.2.genesis 文件中的 id 参数
 - ✓ `sed -i "s/id=1/id=2/g" node0/conf/group.2.genesis`
- 验证是否修改成功
 - ✓ `cat node0/conf/group.2.genesis | grep "id"`

```
$ sed -i "s/id=1/id=2/g" multi_nodes/127.0.0.1/node0/conf/group.2.genesis
$ cat multi_nodes/127.0.0.1/node0/conf/group.2.genesis | grep "id="
  id=2      修改成功
```


搭建并行多组FISCO BCOS区块链

- 依次将node0中修改完的群组2的配置文件拷贝到其余节点
 - ✓ `cp node0/conf/group.2.genesis node1/conf/group.2.genesis`
 - ✓ `cp node0/conf/group.2.ini node1/conf/group.2.ini`
 - ✓ `cp node0/conf/group.2.genesis node2/conf/group.2.genesis`
 - ✓ `cp node0/conf/group.2.ini node2/conf/group.2.ini`
 - ✓ `cp node0/conf/group.2.genesis node3/conf/group.2.genesis`
 - ✓ `cp node0/conf/group.2.ini node3/conf/group.2.ini`

搭建并行多组FISCO BCOS区块链

- 重启节点

➤ 命令: `bash stop_all.sh && bash start_all.sh`

```
$ bash stop_all.sh && bash start_all.sh
try to stop node0
try to stop node1
try to stop node2
try to stop node3
stop node1 success.
stop node2 success.
stop node0 success.
stop node3 success.
try to start node0
try to start node1
try to start node2
try to start node3
node3 start successfully
node2 start successfully
node1 start successfully
node0 start successfully
```

节点重启成功

搭建并行多组FISCO BCOS区块链

● 检查节点共识

- 查看node0共识: `tail -f multi_nodes/127.0.0.1/node0/log/log* | grep +++`

```
$ tail -f multi_nodes/127.0.0.1/node0/log/log* | grep +++
info|2022-04-22 09:32:39.326476|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:32:39.327800|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:32:42.362989|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

此时node0在群组1和群组2中都有共识

- 查看node1共识: `tail -f multi_nodes/127.0.0.1/node1/log/log* | grep +++`

```
$ tail -f multi_nodes/127.0.0.1/node1/log/log* | grep +++
info|2022-04-22 09:29:18.363877|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:29:18.384122|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:29:18.539780|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

此时node1在群组1和群组2中都有共识

搭建并行多组FISCO BCOS区块链

● 检查节点共识

- 查看node2共识: `tail -f multi_nodes/127.0.0.1/node2/log/log* | grep +++`

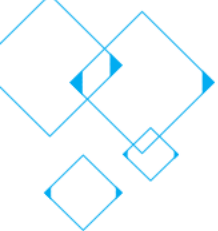
```
$ tail -f multi_nodes/127.0.0.1/node2/log/log* | grep +++
info|2022-04-22 09:31:00.483973|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:31:04.517980|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:31:08.561123|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

此时node2在群组1和群组2中都有共识

- 查看node3共识: `tail -f multi_nodes/127.0.0.1/node3/log/log* | grep +++`

```
$ tail -f multi_nodes/127.0.0.1/node3/log/log* | grep +++
info|2022-04-22 09:31:50.864260|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:31:54.925178|[g:2][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
info|2022-04-22 09:31:58.962314|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=1,tx=0,nodeIdx=0
```

此时node3在群组1和群组2中都有共识



CONTENTS

章节

第三章 国密版FISCO BCOS搭建

3.1 区块链中的密码学

3.2 国密版FISCO BCOS介绍

3.3 搭建国密版FISCO BCOS区块链



区块链中的密码学

- 安全是信任的保障，算法则是安全的基础，节点通信信道的建立、签名的生成、数据的加密等，都需要用到密码学的相应算法。在区块链中，一般使用密码学的场景有以下几种：
 - **数据哈希算法**
 - ✓ 哈希函数是一类单向函数，作用是将任意长度的消息转换为定长的输出值，具有单向性、无碰撞性、确定性、不可逆的性质。在区块链中，哈希函数用于将消息压缩成定长的输出，以及保证数据真实性，确保数据未被修改。
 - **消息签名和验证**
 - ✓ 在区块链中，需要对消息进行签名，用于消息防篡改和身份验证。如节点共识过程中，需要对其他节点的身份进行验证，节点需要对链上交易数据进行验证等。

区块链中的密码学

➤ 数据的加密和解密

- ✓ 加解密算法又分为对称加密和非对称加密两种：
- ✓ 对称加密具有速度快、效率高、加密强度高等特点，使用时需要提前协商密钥，主要对大规模数据进行加密，如FISCO BCOS的节点数据落盘时进行的加密。
- ✓ 非对称加密具有无需协商密钥的特点，相较于对称加密计算效率较低，存在中间人攻击等缺陷，主要用于密钥协商的过程。

➤ 节点TLS握手

- ✓ 节点建立连接时需要使用到密码组件和数字证书，其都需要使用到相应的密码学算法。

国密版FISCO BCOS介绍

- 国密算法由国家密码局发布，包含SM1\ SM2\ SM3\ SM4\等，为我国自主研发的密码算法标准。为了充分支持国产密码学算法，金链盟基于国产密码学标准，实现了国密版的加解密、签名、验签、哈希算法、国密SSL通信协议，并将其集成到FISCO BCOS平台中，实现了对国家密码局认定的商用密码的完全支持，主要有如下替换：
 - 节点TLS握手中采用国密SSL算法；
 - 交易签名生成，验证过程采用国密SM2算法；
 - 数据加密过程中采用国密SM4算法；
 - 数据摘要算法采用国密SM3算法。

国密版FISCO BCOS介绍

- 国密版与标准版FISCO BCOS算法差异

模块名称	标准版FISCO BCOS	国密版FISCO BCOS
SSL链接	Openssl TLSv1.2协议	国密TLSv1.1协议
签名验证	ECDSA签名算法	SM2签名算法
消息摘要算法	SHA-256 SHA-3	SM3消息摘要算法
落盘加密算法	AES-256加密算法	SM4加密算法
证书模式	OpenSSL证书模式	国密双证书模式
合约编译器	以太坊solidity编译器	国密solidity编译器

国密版FISCO BCOS介绍

● SSL连接差异

	OpenSSL	国密SSL
加密套件	采用ECDH、RSA、SHA-256、AES256等密码算法	采用国密算法
PRF算法	SHA-256	SM3
密钥交换方式	传输椭圆曲线参数以及当前报文的签名	当前报文的签名和加密证书
证书模式	AES-256加密算OpenSSL证书模式	国密双证书模式，分别为加密证书和签名证书

国密版FISCO BCOS介绍

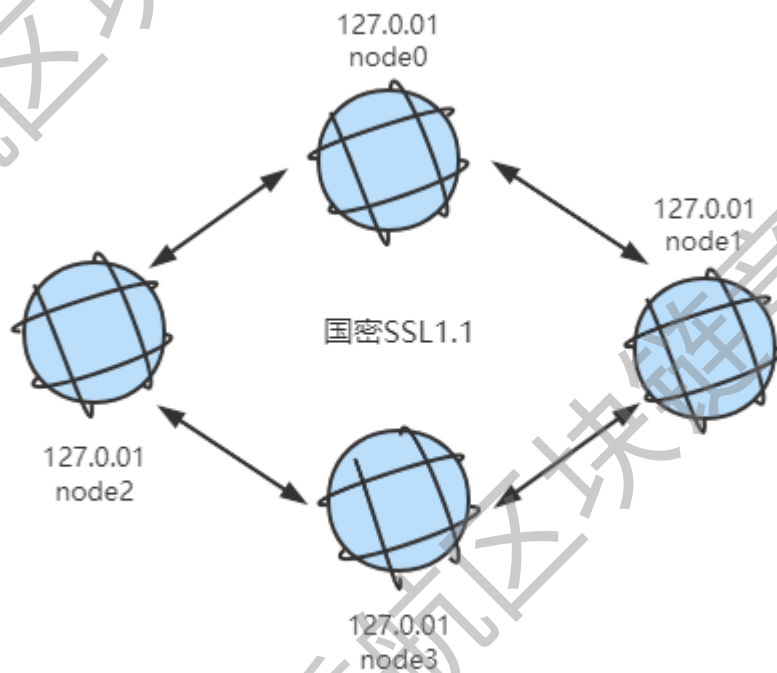
- 国密版与标准版FISCO BCOS在数据结构上的差异

算法类型	标准版FISCO BCOS	国密版FISCO BCOS
签名	ECDSA (公钥长度: 512 bits, 私钥长度: 256 bits)	SM2 (公钥长度: 512 bits, 私钥长度: 256 bits)
哈希	SHA3 (哈希串长度: 256 bits)	SM3 (哈希串长度: 256 bits)
对称加解密	AES (加密密钥长度: 256 bits)	SM4 (对称密钥长度: 128 bits)
交易长度	520bits(其中标识符8bits,签名长度512bits)	1024bits(128字节, 其中公钥512bits,签名长度512bits)

搭建国密版FISCO BCOS区块链

● 场景描述

- 使用开发部署工具搭建一个单机单群组4节点的国密版FISCO BCOS 联盟链。



搭建国密版FISCO BCOS区块链

● 构建国密版FISCO BCOS区块链节点

➤ 构建命令: `./build_chain.sh -l 127.0.0.1:4 30300,20200,8545 -g -G`

```
$ ./build_chain.sh -l 127.0.0.1:4 -p 30300,20200,8545 -g -G
=====
Generating CA key...
Generating Guomi CA key...
=====
Generating keys and certificates ...
Processing IP=127.0.0.1 Total=4 Agency=agency Groups=1
=====
Generating configuration files ...
Processing IP=127.0.0.1 Total=4 Agency=agency Groups=1
=====
[INFO] Start Port      : 30300 20200 8545
[INFO] Server IP       : 127.0.0.1:4
[INFO] Output Dir       : /home/tanniks/fisco/nodes
[INFO] CA Path          : /home/tanniks/fisco/nodes/cert/
[INFO] Guomi CA Path     : /home/tanniks/fisco/nodes/gmcert/
[INFO] Guomi mode        : true
=====
[INFO] Execute the download_console.sh script in directory named by IP to get FISCO-BCOS console.
e.g. bash /home/tanniks/fisco/nodes/127.0.0.1/download_console.sh -f
=====
[INFO] All completed. Files in /home/tanniks/fisco/nodes
```

使用国密版本

构建成功

搭建国密版FISCO BCOS区块链

- 启动节点

➤ 命令: `bash nodes/127.0.0.1/start_all.sh`

```
$ bash nodes/127.0.0.1/start_all.sh
```

```
try to start node0
```

```
try to start node1
```

```
try to start node2
```

```
try to start node3
```

```
node2 start successfully
```

```
node0 start successfully
```

```
node3 start successfully
```

```
node1 start successfully
```

节点启动成功

搭建国密版FISCO BCOS区块链

- 国密版FISCO BCOS有两套证书，一套国密版证书和一套标准版证书，节点与SDK之间既支持SSL连接进行通信，也支持国密SSL连接进行通信。

- 查看国密版证书：ls nodes/127.0.0.1/node0/conf

```
$ ls nodes/127.0.0.1/node0/conf
```

gmca.crt	gmennode.crt	gmennode.key	gmnode.crt	gmnode.key	gmnode.nodeid	gmnode.serial
group.1.genesis	group.1.ini	origin_cert				

国密版证书

原始证书目录

- 查看节点进程

```
$ ps -ef | grep -v grep | grep fisco-bcos
```

进程ID	进程名	命令
45338	/root/test/nodes/127.0.0.1/node2/../../fisco-bcos	-c config.ini
45340	/root/test/nodes/127.0.0.1/node1/../../fisco-bcos	-c config.ini
45342	/root/test/nodes/127.0.0.1/node0/../../fisco-bcos	-c config.ini
45344	/root/test/nodes/127.0.0.1/node3/../../fisco-bcos	-c config.ini

节点进程的进程ID

搭建国密版FISCO BCOS区块链

● 检查共识状态

- 查看node0共识: `tail -f nodes/127.0.0.1/node0/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node0/log/log* | grep +++
info|2022-04-26 17:59:58.046185|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
info|2022-04-26 18:59:58.675508|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
info|2022-04-26 20:59:59.333662|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
```

- 查看node1共识状态: `tail -f nodes/127.0.0.1/node1/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node1/log/log* | grep +++
info|2022-04-26 22:59:59.615098|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
info|2022-04-27 01:59:58.091613|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
info|2022-04-27 03:59:58.211891|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=
```

搭建国密版FISCO BCOS区块链

● 检查共识状态

- 查看node2共识状态: `tail -f nodes/127.0.0.1/node2/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node2/log/log* | grep +++
info|2022-04-27 09:59:58.159632|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
info|2022-04-27 10:59:57.987197|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
info|2022-04-27 11:59:58.721051|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
```

- 查看node3共识状态: `tail -f nodes/127.0.0.1/node3/log/log* | grep +++`

```
$ tail -f nodes/127.0.0.1/node3/log/log* | grep +++
info|2022-04-27 06:59:57.535442|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
info|2022-04-27 07:59:59.708443|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
info|2022-04-27 08:59:57.903062|[g:1][CONSENSUS][SEALER]+++++++ Generating seal on,blkNum=4,tx=0,nodeIdx=0
```

作业

1. 如何编写如下区块链配置文件？

agencyA: 在127.0.0.1上有两个节点，属于group1

agencyB: 在127.0.0.1上有一个节点，同时属于group1和group2

agencyC: 在127.0.0.1上有两个节点，属于group3

2. 还可以如何构建并行多组网络？

3. 如何查看区块链共识情况？

4. 国密版和标准版FISCO BCOS有什么区别？

课程总结

- 本课程详细介绍了
 - 如何搭建星型拓扑网络节点
 - 如何搭建并行多组网络节点
 - 如何搭建国密版的区块链网络

谢谢