POTOS生产链配置讨论

1. 目标

为安全考虑，需要整体review目前POTOS testnet 和 mainnet的系统配置、链下配置、权限治理。

2. 链上系统配置

目前mainnet和testnet在链上系统配置都是一致的。

2.1 链上系统配置现状

节点的二进制版本为：

```
FISCO BCOS Version : 3.10.3
Build Time         : 20240919 14:56:05
Build Type         : Linux/g++/Release
Git Branch         : HEAD
Git Commit         : 5c3f4599d2e6e3d46fece5ab421f8fcdc6d107f3
```

从testnet链观察节点上拉取的配置如下：

Bugfix 默认全开启，不再讨论

Config	Value	Enable Block
auth_check_status	1	0
compatibility_version	3.10.2	113
consensus_leader_period	1	0
feature_balance	1	13
feature_balance_policy1	1	15
feature_balance_precompiled	1	14
feature_dmc2serial	null	0
feature_evm_cancun	1	84
feature_paillier	null	0
feature_paillier_add_raw	null	0
feature_rpbft	null	0
feature_rpbft_epoch_block_num	null	0
feature_rpbft_epoch_sealer_num	null	0
feature_sharding	null	0
tx_count_limit	1000	0
tx_gas_limit	3000000000	0
tx_gas_price	0x5208	86
web3_chain_id	20200	18
balance_transfer	1	114

testnet的创始块内容如下：

```
[chain]
    ; use SM crypto or not, should nerver be changed
    sm_crypto=false
    ; the group id, should nerver be changed
    group_id=group0
    ; the chain id, should nerver be changed
    chain_id=wbininnerchain

[consensus]
    ; consensus algorithm now support PBFT(consensus_type=pbft)
    consensus_type=pbft
    ; the max number of transactions of a block
    block_tx_count_limit=1000
    ; in millisecond, block consensus timeout, at least 3000ms
    consensus_timeout=3000
    ; the number of blocks generated by each leader
    leader_period=1
    ; the node id of consensusers
    node.0=[nodeid1]:1
    node.1=[nodeid2]:1
    node.2=[nodeid3]:1
    node.3=[nodeid4]:1

[version]
    ; compatible version, can be dynamically upgraded through setSystemConfig
    ; the default is 3.2.0
    compatibility_version=3.10.0
[tx]
    ; transaction gas limit
    gas_limit=3000000000
[executor]
    ; use the wasm virtual machine or not
    is_wasm=false
    is_auth_check=true
    auth_admin_account=0xa9c3619f3b8c987bf7aec018814eeb655e45cbbf
    is_serial_execute=true
```

2.2 链上系统配置讨论点

2.2.1 tx_count_limit

该配置控制了区块中的交易上限，是否需要根据链上经济考虑tx_count_limit的上限设置？tx_count_limit应该比区块gaslimit / 21000 更大一点。

目前tx_count_limit还是用的默认值1000.

2.2.2 tx_gas_limit

该配置控制了区块链中交易使用gas的上限。该配置应该比常见合约使用的gas数更高。

典型举例，常见合约使用接口耗费的gas：

- stableCoin（ERC20） transfer：33,848
- ERC721 transfer: 62,243
- ERC721 mint : 103,589
- ERC1155 transfer : 81,848
- Uniswap redeem: 200,625
- Uniswap withdraw: 907,751

目前以太坊的一个区块gasLimit Ethereum Average Gas Limit Chart | Etherscan 大概在3000万左右。参考 https://etherscan.io/chart/tx 的10月23日数据：区块数7175，交易数1137763，区块平均交易数为158。根据 Ethereum Daily Gas Used Chart | Etherscan 所述，10月23日，gas使用108450880000，平均交易使用95319 gas。

综上所述，对于POTOS，tx_gas_limit的下限是单笔常见合约接口的gas数，为100万。上限参考极端的例子，一笔交易就用完300万gas，该交易插入了44kb的数据。Ethereum Blocks #967163 | Etherscan

因此tx_gas_limit的合理取值范围是 [1,000,000 , 3,000,000]

此外，由于web3交易都可以自定义交易的gasLimit，目前在FB上还不支持这个操作。所以后续考虑使用交易中的gas limit，若不指定则默认用系统的配置，若交易中指定的gaslimit超出系统配置，则按照系统的算。

2.2.3 tx_gas_price

该值取决于经济系统设计，后续由经济系统设计为准。

2.2.4 web3_chain_id

目前potos的 testnet chain id为20200，为FISCO BCOS一直以来首选配置的端口号。

mainnet的chain id由于其特殊性还未定，目前为0。需要持续推进。

3. 链下节点配置

3.1 链下节点配置现状

链下配置主要为`config.ini`的内容，testnet和mainnet的配置没有太大区别，所以一起讨论

```
[p2p]
    listen_ip=0.0.0.0
    listen_port=[#P2P_PORT]
    ; ssl or sm ssl
    sm_ssl=false
    nodes_path=./
    nodes_file=nodes.json
    enable_rip_protocol=false

[certificate_blacklist]
    ; crl.0 should be nodeid, nodeid's length is 128
    ;crl.0=

[certificate_whitelist]
```

```
    ; cal.0 should be nodeid, nodeid's length is 128
    ;cal.0=

[rpc]
    listen_ip=0.0.0.0
    listen_port=[#RPC_PORT]
    thread_count=16
    ; ssl or sm ssl
    sm_ssl=false
    ;ssl connection switch, if disable the ssl connection, default: false
    disable_ssl=true

[web3_rpc]
    enable=[#ENABLE_WEB3_RPC]
    listen_ip=0.0.0.0
    listen_port=8545
    thread_count=8

[cert]
    ; directory the certificates located in
    ca_path=./conf
    ; the ca certificate file
    sm_ca_cert=sm_ca.crt
    ; the node private key file
    sm_node_key=sm_ssl.key
    ; the node certificate file
    sm_node_cert=sm_ssl.crt
    ; the node private key file
    sm_ennode_key=sm_enssl.key
    ; the node certificate file
    sm_ennode_cert=sm_enssl.crt

[security]
    private_key_path=conf/node.pem

[storage_security]
    ; enable data disk encryption or not, default is false
    enable=false
    ; url of the key center, in format of ip:port
    ;key_center_url=
    ;cipher_data_key=

[consensus]
    ; min block generation time(ms)
    min_seal_time=500

[sync]
    allow_free_node=true

[storage]
    data_path=data
    enable_cache=true
```

```
    ; The granularity of the storage page, in bytes, must not be less than 4096 Bytes, the
default is 10240 Bytes (10KB)
    key_page_size=0
    pd_ssl_ca_path=
    pd_ssl_cert_path=
    pd_ssl_key_path=
    enable_archive=false
    archive_ip=127.0.0.1
    archive_port=

[txpool]
    ; size of the txpool, default is 15000
    limit=15000
    ; txs notification threads num, default is 2
    notify_worker_num=2
    ; txs verification threads num, default is the number of CPU cores
    ;verify_worker_num=2
    ; txs expiration time, in seconds, default is 10 minutes
    txs_expiration_time = 600

[redis]
    ; redis server ip
    ;server_ip=127.0.0.1
    ; redis server port
    ;server_port=6379
    ; redis request timeout, unit ms
    ;request_timeout=3000
    ; redis connection pool size
    ;connection_pool_size=16
    ; redis password, default empty
    ;password=
    ; redis db, default 0th
    ;db=0

[flow_control]
    ; the switch for distributed rate limit
    ; enable_distributed_ratelimit=false

    ; rate limiter stat reporter interval, unit: ms
    ; stat_reporter_interval=60000

    ; the module that does not limit bandwidth
    ; list of all modules: raft,pbft,amop,block_sync,txs_sync,light_node,cons_txs_sync
    ;
    ; modules_without_bw_limit=raft,pbft

    ; restrict the outgoing bandwidth of the node
    ; both integer and decimal is support, unit: Mb
    ;
    ; total_outgoing_bw_limit=10

    ; restrict the outgoing bandwidth of the the connection
```

```
    ; both integer and decimal is support, unit: Mb
    ;
    ; conn_outgoing_bw_limit=2
    ;
    ; specify IP to limit bandwidth, format: conn_outgoing_bw_limit_x.x.x.x=n
    ;   conn_outgoing_bw_limit_192.108.0.1=3
    ;   conn_outgoing_bw_limit_192.108.0.2=3
    ;   conn_outgoing_bw_limit_192.108.0.3=3
    ;
    ; default bandwidth limit for the group
    ; group_outgoing_bw_limit=2
    ;
    ; specify group to limit bandwidth, group_outgoing_bw_limit_groupName=n
    ;   group_outgoing_bw_limit_group0=2
    ;   group_outgoing_bw_limit_group1=2
    ;   group_outgoing_bw_limit_group2=2

[log]
    enable=true
    ; print the log to std::cout or not, default print to the log files
    enable_console_output = false
    log_path=[#LOG_PATH]
    ; info debug trace
    level=info
    ; MB
    max_log_file_size=512
    ; LineID, TimeStamp, ProcessID, ThreadName, ThreadID and Message
    format=%Severity%|wbbc-occnode|7857|%TimeStamp%|%ThreadName%-%ThreadID%|%Message%
    enable_rotate_by_hour=false
    log_name_pattern=wbbc-occnode.log
    ; Y,m,d,H,M,S are supported, N is the sequence number log_%Y%m%d.%H%M%S.%N.log
    rotate_name_pattern=wbbc-occnode_%Y%m%d.%H%M.log
    ; if archive_path is empty, the archive function will be disabled
    ; archive_path=./log/
    compress_archive_file=true
    ; ; 0: no limit, in MB
    ; max_archive_files=10
    ; ; 0: no limit, in MB
    ; max_archive_size=0
    ; min_free_space=0
```

3.2 链下节点配置讨论项

3.2.1 consensus.min_seal_time

在初期交易少的时候，可以全局降低，以提高出块速度。所有节点的min_seal_time最好是一样，若要不一样则所有节点的min_seal_time最大最小值的差值要小于`consensus_timeout`

3.2.2 sync.allow_free_node

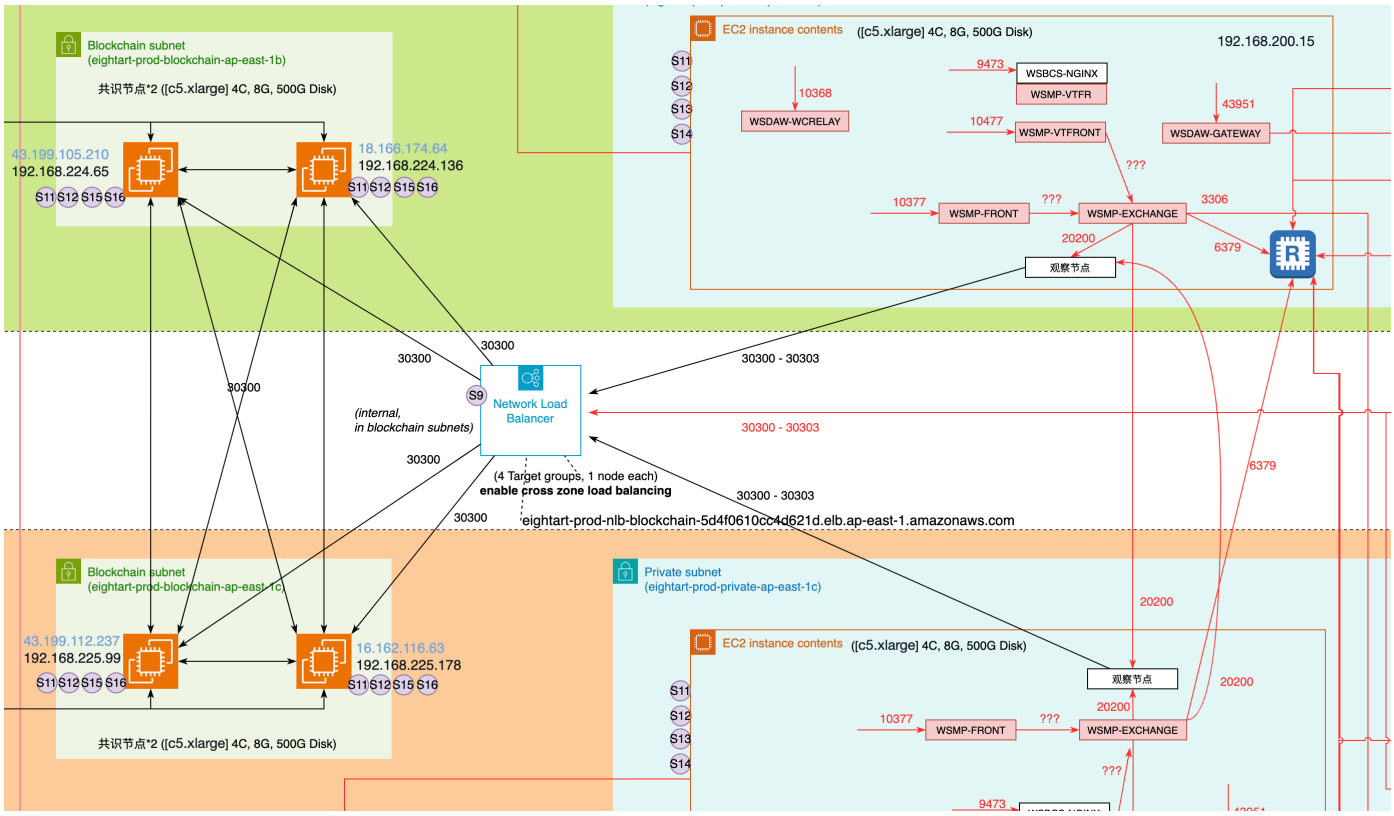
该配置可以允许游离节点同步区块。该配置在testnet是打开的，在mainnet是关闭的。

3.2.3 txpool.limit

考虑到potos生产的机器都是4c8g，所以先维持现状

4. 共识节点配置

目前testnet和mainnet的节点配置均为4个共识节点2个观察节点。共识节点之间直接用ip互联，在public区。观察节点通过Network Load Balancer（NLB）连接到共识节点，在private区。



5. 权限管理

目前testnet和mainnet都开启了权限控制。所以所有关于链上系统配置的修改都需要用治理委员的形式处理。

治理委员原理参考：权限治理体系设计 操作手册参考：权限治理使用指南

对于mainnet目前只有一个治理委员，其密钥保管在运维。

对于testnet目前由三个治理委员，每个治理委员的权重为1，任何治理委员均可发起修改系统配置的proposal，所有密钥也保管在运维。

```
-------------------------------------------------------------------------------------------------
---
Committee address   : 0x1546453e7a9e387f8f17da575cdd54d846f0ff1e
ProposalMgr address : 0x852bd1469b51f8e538adb5107428983c9cef0387
-------------------------------------------------------------------------------------------------
---
ParticipatesRate: 0% , WinRate: 0%
-------------------------------------------------------------------------------------------------
---
Governor Address                                          | Weight
index0 : 0xa9c3619f3b8c987bf7aec018814eeb655e45cbbf       | 1
index1 : 0x8d8151770543314ce1451b4b3c017db4630cb20f       | 1
index2 : 0x48270ae91f4b9c37a0371112a4a5e691b5b46936       | 1
```

治理委员 -> 合约管理员 -> 普通用户

治理委员有什么权限?

- 需投票
  - 更改治理委员会投票阈值
  - 更改某个治理委员的权重
  - 剔除某个治理委员
  - 更改计算模板
  - 决定部署合约权限
  - 重置某个合约的管理员
  - 设置链上系统
  - 更改共识节点、观察节点、节点投票权重
- 无需投票
  -