目录

CONTENTS

一、设计详述

QOS目的是建立适用于企业级应用的区块链底层公链，满足行业内各细分场景的独立性和交互性，所以我们不是设计区块链基础协议，而是专注于权益记录和转移的区块链网络。

1.1 角色

QOS网络有三类参与角色 :业务参与者、服务提供者、QOS基础验证人。

- 业务参与者

业务参与者是一群权益所有者，他们使用服务提供者提供的基于联盟链的区块链服务。

- 服务提供者

服务提供者提供各类服务供权益所有者使用，这些服务以业务链方式提供。

- QOS基础验证人

QOS基础验证人在QOS基础链里打包新区块，每个QOS基础验证人必须在高可用和高带宽的机器上运行一个QOS节点。

1.2 共识

业务链主要是以联盟链或私有链方式提供服务，使用拜占庭容错共识算法(BFT)。

QOS基础链借鉴Tendermint共识协议，采用BFT+DPOS混合型共识算法。QOS基础链的基础验证人必须是专门用来提交区块的超级节点，基础验证人通过QOS代币来进行权益认证和激励，通过BFT算法避免单节点作恶。

1.3 双层链架构

QOS是一个可伸缩双层链系统，分为独立的业务链和解决业务链互操作的QOS基础链。

QOS基础链提供全网的身份体系、共识算法体系、智能合约体系、基础代币与业务代币发行体系。

业务链可以采用联盟链或私有链方式通过使用拜占庭容错共识算法来运行，每个业务链可以在自己的账本中记录各自的代币状态。

QOS基础链通过中继协议方式支持各业务链交互，以便各业务链间安全快速的进行价值交换。QCP（QOS Constellation Protocol)是QOS的跨链协议，协议基于队列机制和梅克尔树证明（Merkle Proof）实现。

QSC协议是符合QOS公链标准的，基于智能合约的代币发行与运营协议。开发者基于QSC协议可以在QOS上实现自己的自治组织，由于开发者遵循统一QSC协议，因此能安全的实现价值互转。

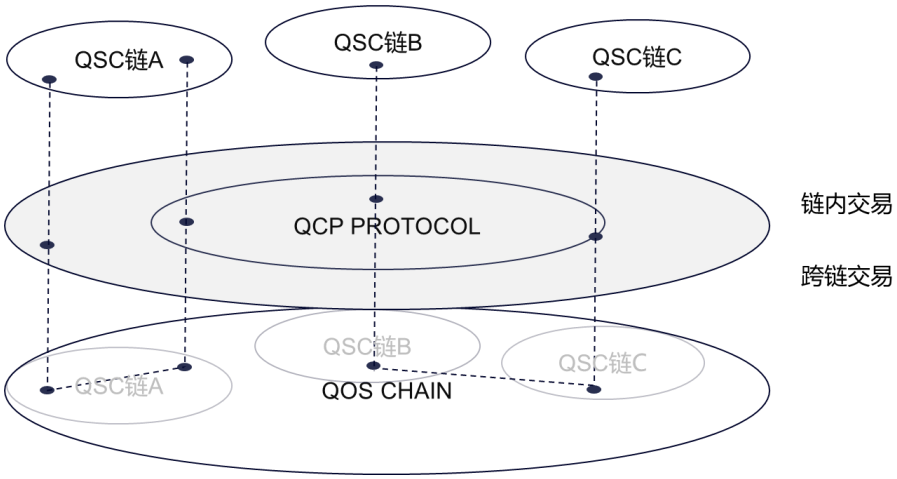


图2.1 QOS双层链架构

QOS基础链以中继协议的方式运行，承载的是多资产分布式账本，状态信息包含QOS基础链状态和各业务链的代币状态。

QOS基础链支持基于QSC协议部署公链智能合约，同时会内置一些特殊合约（共识合约、验证人合约、跨链合约等）来支持跨链共识交易，另外会提供跨链管理合约来支持跨链协议的升级，跨链合约封装为gRPC服务以简化业务链调用跨链交易。

业务链是独立的区块链，业务链之间通过QOS基础链以QCP协议通信。

1.4 跨链协议

解决公链和联盟链之间的跨链交易问题，前提是公链和联盟链都要符合一定约定，本技术把这种约定整理成一种协议叫做QCP跨链协议，cassini是本技术的一种具体实现。

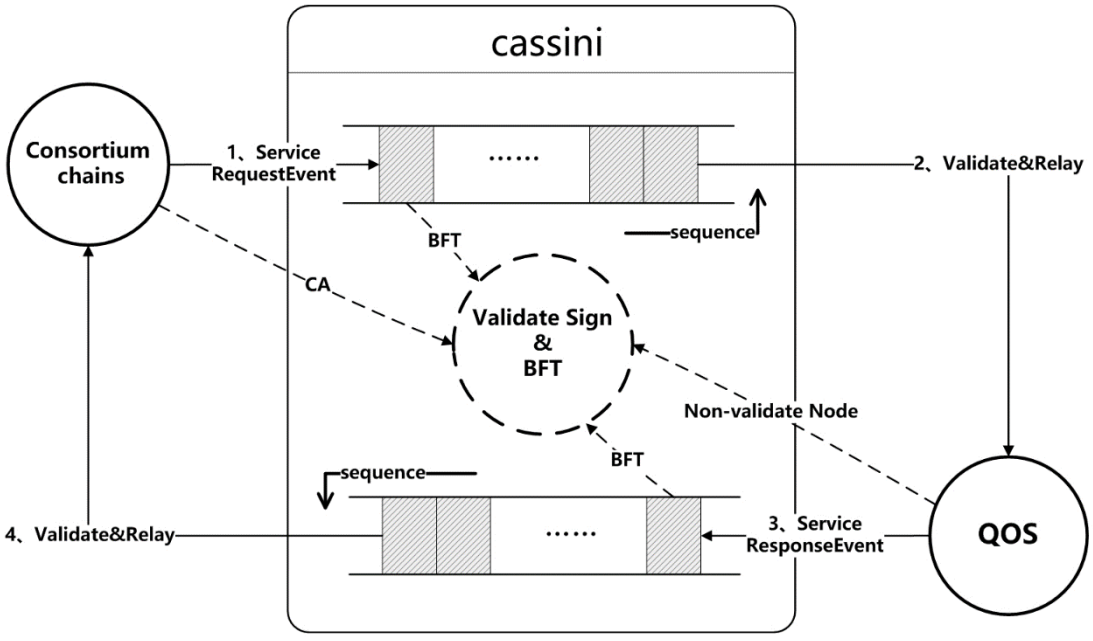


图2.2 QOS双链通信机制

有若干个cassini节点连接联盟链（consortium）和公有链(QOS)，cassini持有联盟链ca颁发的证书，联盟链节点持有cassini公钥，可以识别cassini身份。多个cassini节点之间进行BFT共识，防止个别cassini节点作弊。

QCP协议：

QOS和任意遵循QCP协议的Blockchain连接共同的中继Cassini；

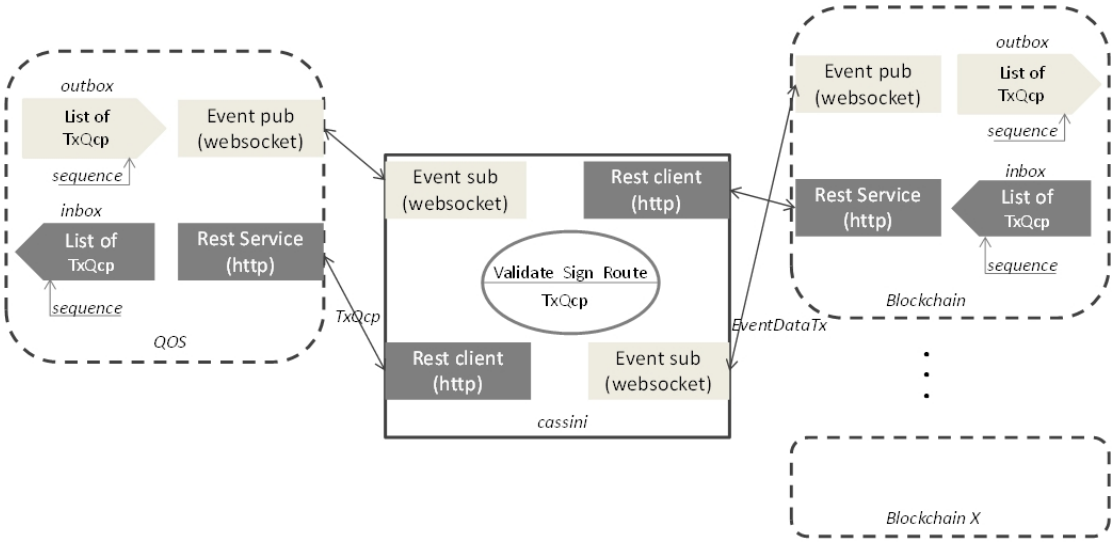
Cassini订阅链上跨链交易事件，获取交易摘要，进行2/3共识，随机找一个诚实节点获取跨链交易；

当QOS新块内有跨链交易，将跨链交易放入outbox,并按顺序递增编号，当前最大编号叫sequcnce。区块链保证该编号的连续性；

Blockchain将通过Cassini收到的交易存入inbox；

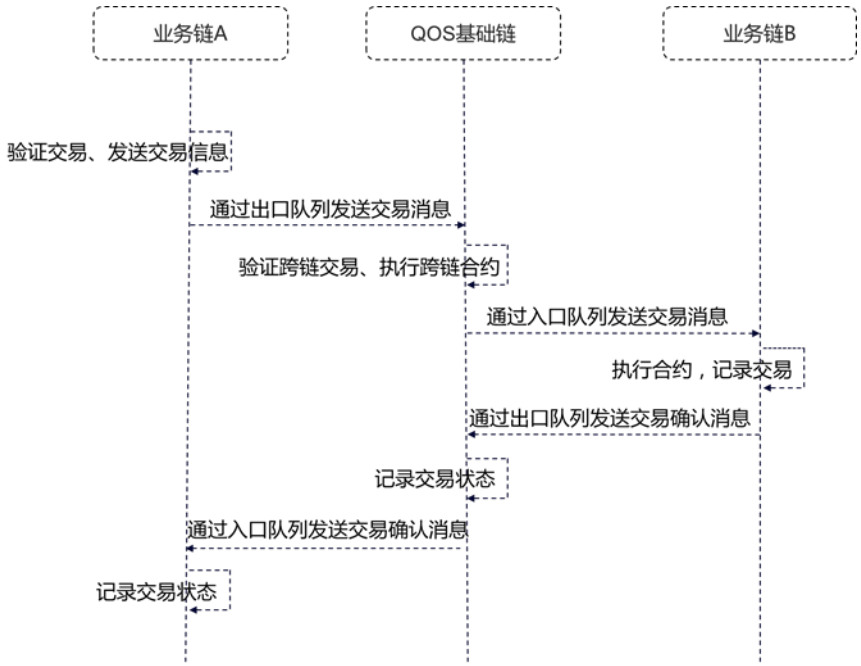
Cassini查询Blockchain inbox 的sequence 记作seq1,中继顺序取QOS的 outbox 的编号大于seq1的交易，一次可以取一条或多条；

Cassini 对交易进行验签，2/3 共识等处理后路由到目标链；



1.5 跨链交易

跨链交易通过在业务链上增加两个先进先出的队列机制解决，队列通过梅克尔树证明（Merkle Proof）来保证数据真实。



跨链交易详细步骤：

Cassini监听链上跨链event。

链将跨链的交易在结构体 ResponseDeliverTx成员变量Tags中增加值对“qcp.to = 'xxx' “ 。XXX表示目标链的名称。

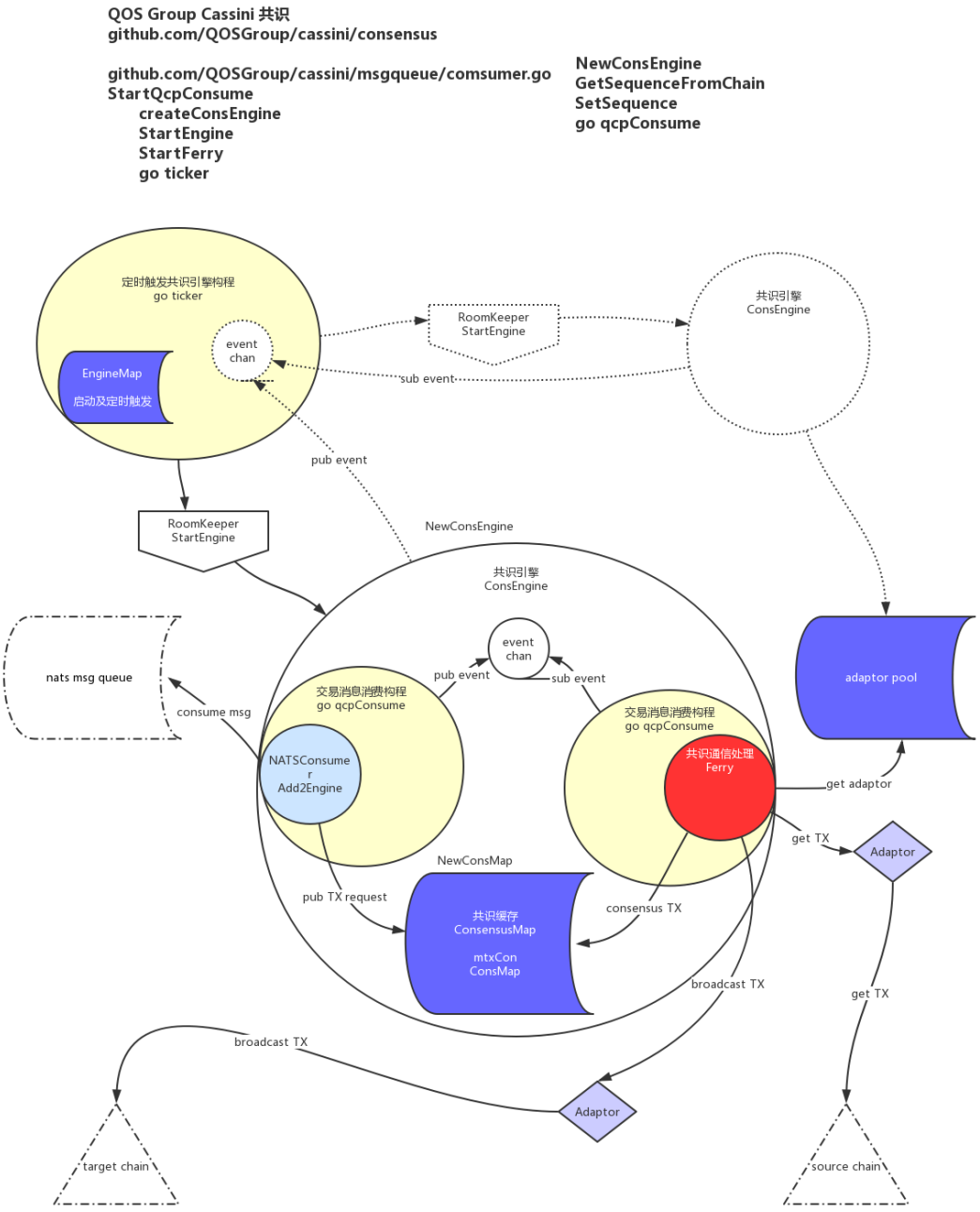
Cassini收到事件后，会进行2/3 的共识校验。

通过2/3 共识校验后，Cassini会进一步调用restful API（ABCI Query）查询交易数据。

Cassini查询到交易数据，在Cassini节点间进行BFT共识，然后通过调用restful API（ABCI BroadcastTxAsync 或ABCI BroadcastTxSync）向目标链提交交易，完成交易的处理。

跨链交易结果返回过程同a,b,c,d,e步。

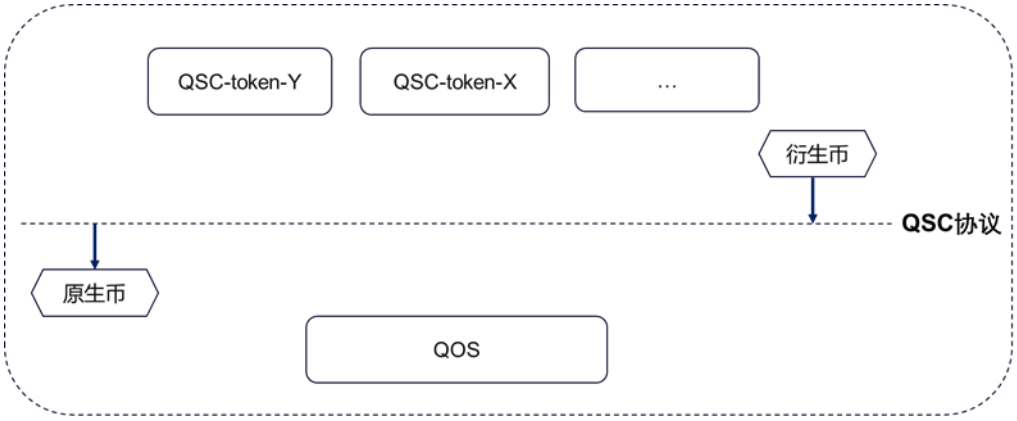
cassini的代码框架：



该框架采用了adapter模式，从而可以扩展兼容其它链，包括未来的区块链，只要该链兼容QCP协议就可以。

1.6 QOS双层代币体系

QOS公链有原生币QOS，也可以通过智能合约创造衍生币。原生币只有一种，衍生币可以有多种。衍生币执行QSC协议标准。



衍生币的计算机表示：

```
struct token{amount uint,id uint}
```

QSC标准：

```
contract QSCInterface {
    string public constant name = "Token Name";
    string public constant symbol = "SYM";
uint8 public constant decimals = 0;
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint balance);
    function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool success);
    function transferFrom(address from, address to, uint tokens) public returns (bool success);
    function frozenAmount(address tokenOwner) public returns (uint frozentokens);
    function frozen(address tokenOwner, uint tokens) public returns (bool success);
```

```
        function unfrozen(address tokenOwner, uint tokens) public returns (bool success);

        event Transfer(address indexed from, address indexed to, uint tokens);

        event Approval(address indexed tokenOwner, address indexed spender, uint tokens);

        event Frozen(address indexed tokenOwner, uint tokens);


    //option. the contract owner use this function to pause the contract
    function pause() public returns (bool success);
    //base on QCP protocol, implement info exchange between chains
    function qcpExchange() public returns (bool success);
    }
```

QSC标准说明：

类型	名称	说明
静态变量	name	币的完整名称。
	symbol	币的符号，例如QOS、ETH等。
	decimals	小数点位数。
函数功能	totalSupply	发行币的总量。
	balanceOf	获取指定地址币的余额。
	transfer	调用transfer函数将自己的token转账给to地址，value为转账个数。
	approve	批准spender账户从自己的账户转移value个token。可以分多次转移。
	transferFrom	与approve搭配使用，approve批准之后，调

		用transferFrom函数来转移token。
	allowance	返回spender能提取token的个数。
	frozen	冻结一定数额token。
	unfrozen	解冻一定数额token。
	frozenAmount	获得指定账户当前被冻结的token总额。
	pause	暂停该合约所有调用。由合约所有者在特殊情况下调用，以便解决bug并止损。
	qcpExchange	基于QCP协议，实现跨链的信息交互。
事件	Transfer	当成功转移token时，触发Transfer事件。
	Approval	当调用approval函数成功时，触发Approval事件。
	Frozen	当调用frozen函数成功时，触发Frozen事件。

QSC协议兼容ERC20标准，在ERC20代币可以流通的地方QSC代币技术上也可以流通，这样QSC代币更容易对接多个平台。

以两种QSC代币X-token和Y-token之间兑换为例，共需要两步如下图：

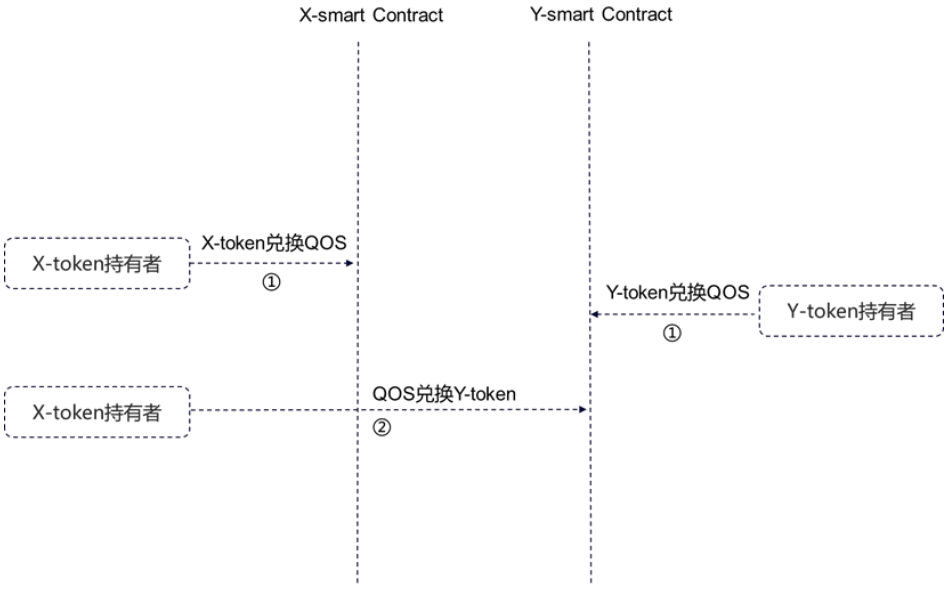


图2.5 QSC协议代币之间兑换流程

QOS公链中X-token要兑换成QOS公链之外的代币比如以太币 ,那么交易过程共三步：

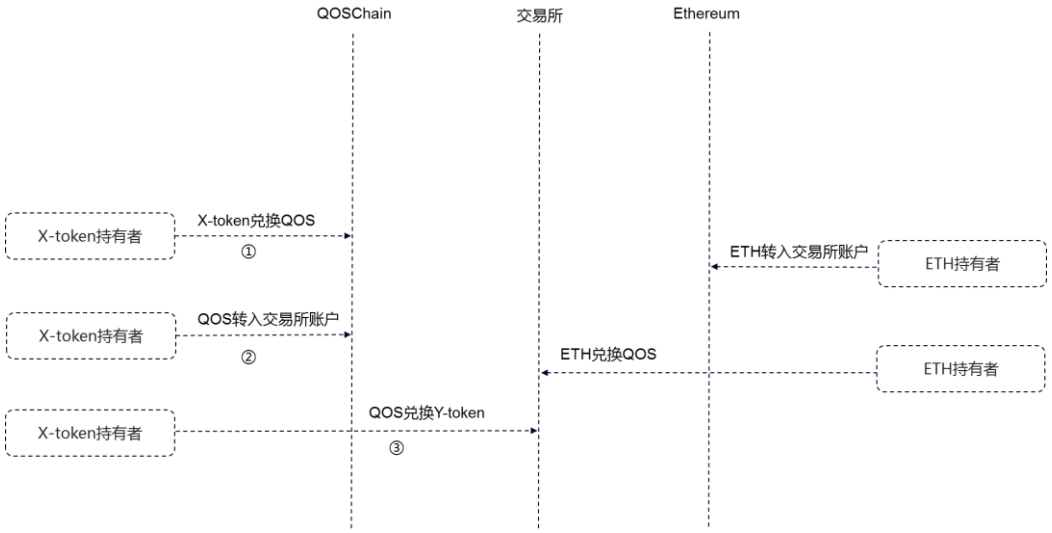


图2.6 QSC协议代币与QOS公链外代币交易流程

二、QOS验证委托经济模型

QOS公链代币总量100亿枚，其中49%在QOS公链初始化时由早期发行的ERC20代币在创世区块中兑换产生，51%在QOS公链上由超级节点挖矿产生。每隔一个时间周期T铸币速度减半，并规定7个时间周期铸币完成，第七个周期与第六周期铸币速度相等，每个区块生成块的阈值预设为达到3秒。

T时间内挖矿产生的QOS币总量$\approx \frac{100亿 * 51\%}{2^{\mu}}$

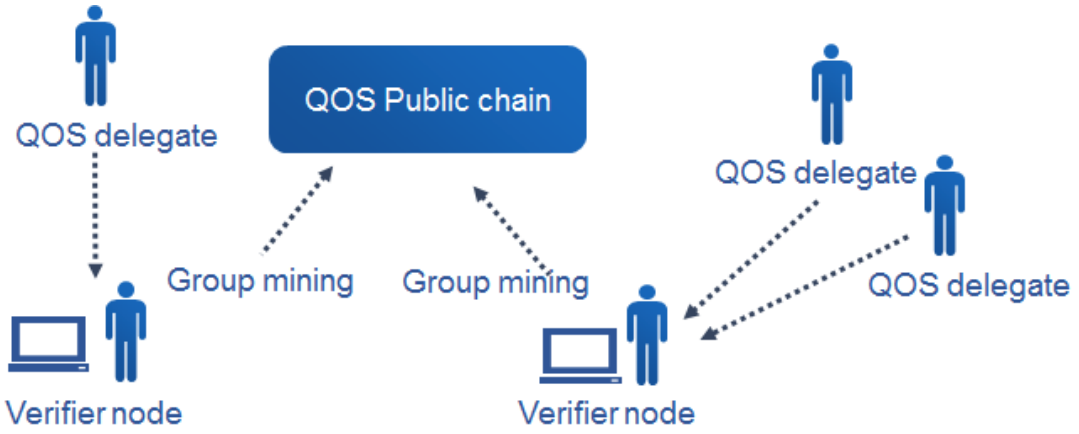
μ= 取整$(\frac{当前时间-QOSChain初始时间}{T})$

当T为4年，那么QOS币在约28年后被挖完。

表2.1 QOS挖矿机制

时间	第1个四年	第2个四年	第3个四年	第4个四年	第5个四年	第6个四年	第7个四年
新铸币QOS数量（亿枚）	25.5	12.75	6.375	3.1875	1.59375	0.796875	0.796875
新区块奖励QOS数量（枚）	60.64	30.32	15.16	7.58	3.79	1.895	1.895

QOS公链是基于授权股权证明Delegated Proof-of-Stake和拜占庭容错共识算法的双层链机制的区块链基础设施。QOS公链的挖矿数额是按年度固定的，在主网上线的第一年内，每产生一个区块产生的QOS数量大体相同，网络中的全部活跃的验证人都可以依据其绑定的QOS数量占网络中总的绑定QOS的比例获得挖矿收益。

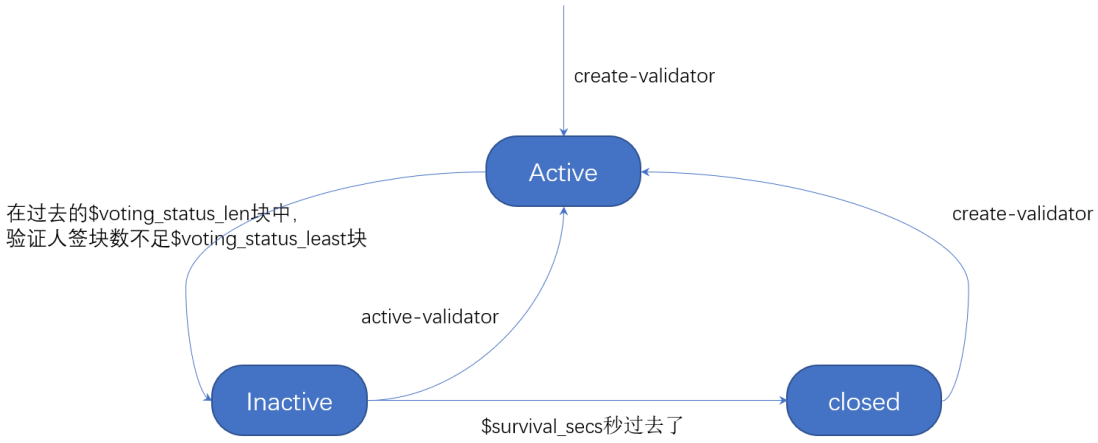


2.1 验证人（Validator）

QOS公链中有一个验证人节点的集合，验证人节点担当了BFT共识算法的具体实现——网络中的每一块都需要收集至少2/3的验证人节点签名。QOS公链中的每一块包含零到多条交易，验证人节点对块中的交易进行校验，对校验通过的块用自己的私钥签名，并广播到网络中去。

QOS公链验证人节点通过绑定一定的QOS，同时承担了DPOS算法的实现——依照其绑定的QOS数量，获得QOS网络挖矿的收益。

2.1.1 验证人节点的几种状态



- 活跃状态

保持不间断地验证区块交易，以私钥签名并广播的状态。 普通全节点，通过发出 create-validator 交易，可能转为活跃状态。

但并非任意全节点都可以通过以上方式成为活跃验证人 ,由于网络限制了总验证人数量，在一个特定时间，QOS 网络以过去的$voting_status_len 个块中，验证过并有签名的块数至少要达到$voting_status_least，来明确一个验证人节点是否活跃。我们称$voting_status_len 为验证人保活窗口。

例如，测试网中的保活窗口宽度$voting_status_len=1000，最小保活块数$voting_status_least=500

如果验证人未能达到这个要求，将被强制切换到非活跃状态。

一个新创建或者重新激活的验证人，如果经历的总块数尚不足窗口宽度，但漏签块数已达$voting_status_least，也将被切换到非活跃状态

活跃状态的验证人，可以进行区块验证，可以提交区块，获得挖矿收益，可以通过达成代理合约获得收益，也可以获得交易费用。

- 非活跃状态

由于未达到活跃窗口要求 ,或者通过发出 revoke-validator 交易主动要求，验证人将转为非活跃状态。非活跃状态是验证人从活跃状态到退出状态之间所必须经历的中间态。

非活跃状态最久能够维持观察期即$survival_secs 秒 ,非活跃的验证人如果什么都不做，经过$survival_secs 后将自动退出，失去其验证人身份。

非活跃状态的验证人，不能进行区块验证，不能提交区块，不能获得挖矿收益和交易费用，不能达成代理合约，需要渡过观察期退出后，通过代理合约绑定的 QOS 才能回到投资者账户上。

- 退出状态

退出状态的验证人将其上绑定的 QOS 自动返还给各投资者，自绑定的部分也会回到验证节点的所有者（owner）账户上。

退出后的验证人的权益与普通节点无异。

2.1.2 验证人节点的权重（voting power）

作为一个 DPOS 区块链网络，QOS 网络中的验证人节点需要绑定一定量的 QOS 来构成其权益。

QOS 目前规定验证人必须有一定的自绑定 QOS 来初始化运行验证人节点。创建后，其绑定的 QOS 可以来自于验证人所有者(owner)自己的账户，在 createValidatorTX 初始化时绑定，或者后期再绑定给自己（*后续版本*）；也可以通过发布和签订代理合约（delegation contract），来吸纳不具备代理人资格的节点的投资（*后续版本*）。

- 参与挖矿收益的分配：

每出一个新块时，验证人的权重决定了其分配挖矿收益的比例，如下：

$$\text{验证人的挖矿收益} = \frac{\text{验证人当前绑定QOS数量}}{\text{全部活跃状态验证人绑定QOS数量之和}} \times \text{该块新挖QOS数}$$

- 社区自治的话语权：

进行社区自治投票时，验证人的权重决定其决定的话语权比例。但普通节点也有社区自治的投票权，当验证人绑定的 QOS 来自普通节点的委托协议时，投资者的意志将覆盖验证人这部分权重。

2.1.3 QOS公链代理机制

对于没有能力成为验证人的节点，也将可以通过将其账户中的 QOS 委托给验证人的方式获得挖矿收益。

每个 QOS 验证人将可以发布一系列的委托合约，合约规定委托人通过将 QOS 在一定时间段内交予验证人作为绑定的 QOS 参与挖矿，获得的收益如何分配。

加入测试网络，申请成为验证人：
http://docs.qoschain.info/qos/install/testnet.html

三、用户接入

3.1 轻节点客户端

由于区块链的去中心化的特点，存在成千上万的全节点（full node）同步保存着链上的所有区块信息。随着时间的推移，区块链上的交易会越来越多，并造成了区块链上的数据越来越大，全节点（full node）必然需要耗费大量的包括存储，带宽在内的计算机资源来同步链上的全量数据。当用户在移动端手机利用分布式 App 软件应用（DApp）想要接入到区块链上从事交易操作，例如获取链上的交易信息，按照现有的区块链（例如比特币）方案，需要通过自己搭建的区块链全节点（full node）或者通过第三方提供的代理节点来执行。

整个交易过程中，全节点（full node）作为区块链的入口，关系整个端到端交易过程的安全性和可靠性。不论是自建的还是第三方指定的全节点（full node），从终端用户侧没法验证其所获取的区块链信息的正确性和完整性。全节点（full node）需要耗费大量的计算机资源包括硬件存储，通信带宽等来及时同步区块链上日益增加的全量数据信息。当全节点（full node）由于其他因素限制而没能同步区块链上的数据信息后，或者节点被黑客攻击控制后，就没法给终端用户反馈完整甚至准确的信息。

QOS 采用拜占庭校验算法，提供在移动端植入轻客户端模块，引入了特殊的数据结构来保存区块链的块头。当执行交易操作时，移动手机端会将收到的区块信息的块头与存储在手机上的块头进行对比，具体来说是对比块头数据中的验证人集合。根据拜占庭算法，只有达到 2/3 的超多数时才会形成共识。同样，在比对块头数据中的验证人集合时，只有验证人集合的变化少

于 1/3 时，才可以完成比对校验，确认收到的信息是安全可信的。否则，验证人集合中变化的验证人数量多于 1/3，校验失败，无法直接判断该校验是否安全可靠。需要引用二分法进行下一轮校验：选择本地存储的块头和收到的新块头中间的块头进行校验，如果验证人集合变化小于 1/3，更新本地存储至中间块头信息，再与收到的新块头进行校验…如此反复，最后完成校验过程。

本技术详细步骤：

a) 用户 Alice 在早上 6 点通过手机进行了 1 笔交易转账，当交易信息上链后，断开了网络连接，此时手机里存储的块头验证人集合是（A, B, C, D）；

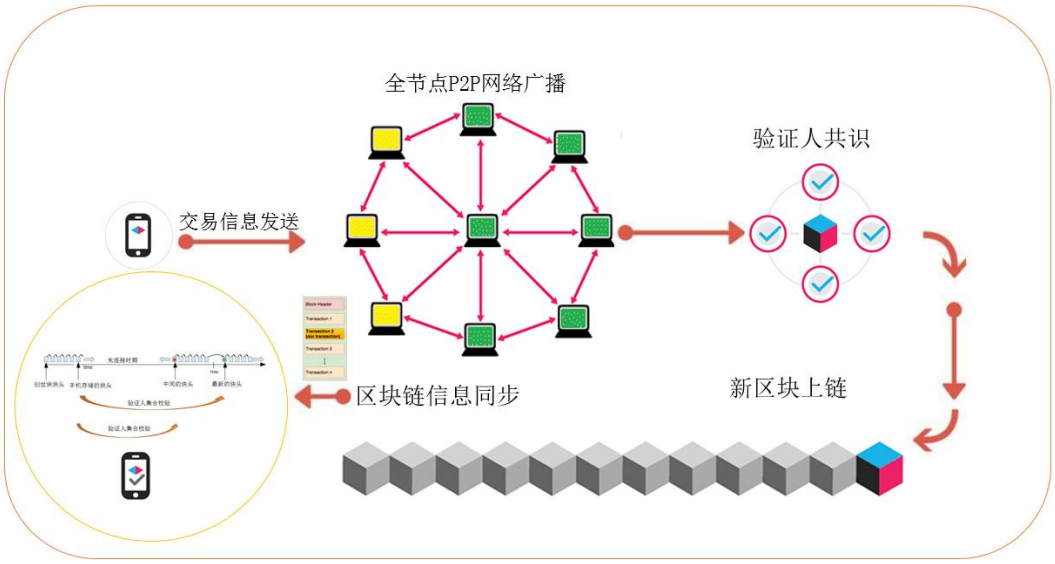
b) Alice 在 12 点连上区块链进行账户查询，链上返回了数据信息，其中最新块头验证人集合是（A, B, E, F）。手机端校验机制启动，由于验证人集合变化大于 1/3，手机没法直接校验通过，需要进行下一轮校验；

c) 手机轻客户端索取更早时间段例如 9 点钟的区块信息，此时块头的验证人集合是（A, B, C, E），验证人集合变化小于 1/3，校验通过，手机端存储新的块头信息，验证人集合为（A, B, C, E），此时再与最新 12 点的块头进行校验，由于验证人集合变化小于 1/3，校验通过，证明收到的最新的信息是安全可靠的，并且更新最新的块头信息存储到手机本地；

d) 当用户在手机上进行下一次区块链交易操作并获得链上数据信息时，首先会比对手机本地与收到的链上块头信息来校验收到信息的安全

和可靠性。

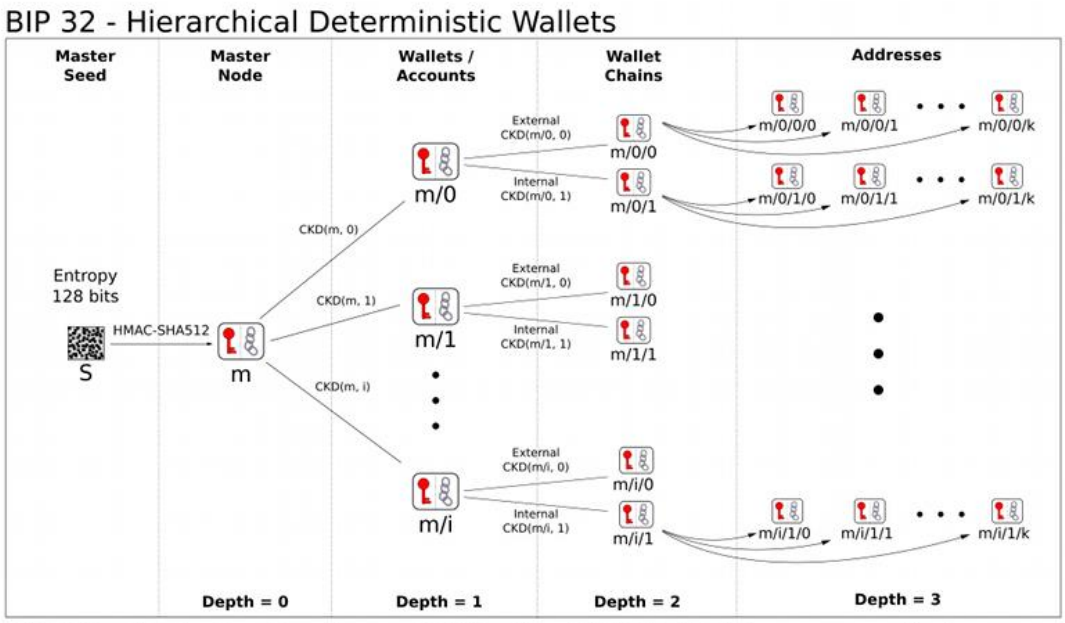
本技术数据流程图如下图所示：



3.2 钱包体系

因为 QOS 公链采取了双链结构，需要实用性地支持商业级别的可伸缩性和隐私性。因此 QOS 公链的数字钱包在 BIP32 以及 BIP44 协议基础上采用了高度灵活的钱包体系设计。

BIP32 协议原理图如下：

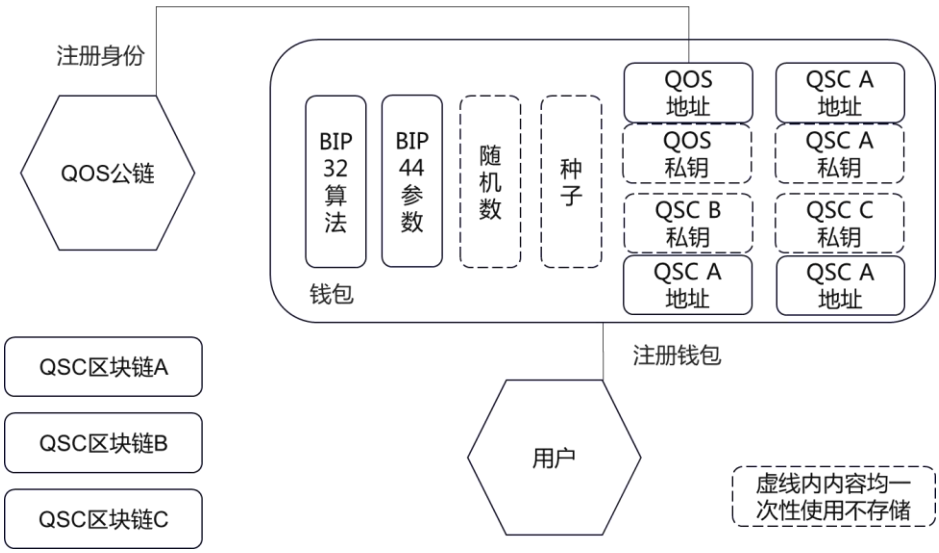


QOS公链钱包将成为QOS的开源项目。申请公链钱包时，钱包客户端采用量子算法生成真随机数，并由用户自行设定产生HDWallet的种子助记词。二者根据BIP32以及BIP44协议生成在QOS公链上使用的地址。用户地址将注册在QOS公链上，作为用户身份的唯一标识。

QOS公链钱包不保存用户私钥。在项目初期，用户自行分别保存真随机数和种子助记词。 钱包进行交易签名时，通过加密通道获取真随机数和种子助记词，一次性计算出私钥，完成签署。

用户在QSC业务链上开展业务时，统一使用QOS公链钱包，根据BIP44协议生成在业务链上的地址和相应签署私钥，流程同上所述。

QOS公链钱包将适时推出硬件钱包，以解决私钥的安全存储问题。QOS公链钱包整体结构如下图所示。



3.3 统一身份认证

一般而言，公民身份往往意指以用户生物学识别特征为基础，以政府认证的身份识别数据为依据，对个人的标识。随着越来越多的社会活动和经济活动从线下向线上的转移，利用虚拟身份进行欺诈的案件越来越多，多平台身份的打通越来越成为业界的关注点。

QOS认为身份不仅仅只是标识，而具有广义的内涵，在QOS社区内，身份包含着多重的含义，例如：

a) 一定情境下的唯一标识，例如在国际社会上的护照、中国境内的身份证、某一个网络社区上的ID，这些标识出于技术、政治、商业等原因往往很难跨情景打通。

b) 地域、种族、宗教、信仰概念，例如区块链从业者经由一种分布式、去中心化的社区理想而走到一起。

c) 社会角色和定位，例如雇员和雇主、父子、同事等，与他人存在的某种关系成就了公民的某个身份。

d) 能力，无论是经济能力、消费能力、身体能力也是身份的一种，奥运冠军就是一种荣耀的身份象征。

e) 信用 ,信用无疑是公民的重要身份之一 ,经由个体的历史借贷情况、履约情况得到体现。

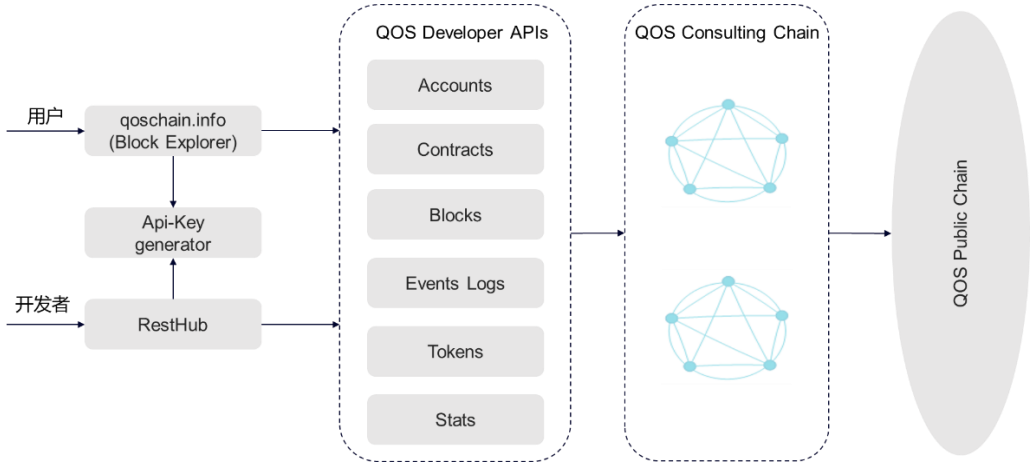
f) 爱好，由爱好促成的社群往往持久而有生命力，个体对于基于爱好产生的社群往往具备更强的归属感，而形成独特的身份特征。

QOS将以上体现公民各个不同维度识别特征的综合定义为广义身份，广义身份跨越国别、语言、互联网，成为每一个个体的唯一标识。

QOS作为通用的企业级应用社区，让无数个场景服务商、数据服务商、钱包服务商、交易所等等基于统一的底层平台向社区公民提供服务，有望形成一个统一身份认证，公民自治，身份信息全面、准确、可控，价值万亿美元以上的社区经济体。

3.5 QOS公链区块链浏览器

QOS公链以社区服务的方式为开发者提供API，方便查看区块链运行信息，同时QOS运营团队，也会基于这些API实现公链区块链浏览器，方便普通用户浏览QOS公链和子链交易状态信息，地址为浏览器。QOS开发者API和区块链浏览器的架构如下图：


用户
qoschain.info
(Block Explorer)
Api-Key
generator
开发者
RestHub
QOS Developer APIs
Accounts
Contracts
Blocks
Events Logs
Tokens
Stats
QOS Consulting Chain
QOS Public Chain

四、联系方式及社群

官网

https://www.qoschain.io

服务邮箱

contact@qoschain.io

Facebook

https://facebook.com/QOS.Foundation

Twitter

https://twitter.com/QOS_Foundation

Telegram

https://t.me/QOSOfficial_EN
https://t.me/QOSOfficial_CN

微博

https://weibo.com/u/6310001987

validator step by step(视频)

https://v.youku.com/v_show/id_XMzk4NzM3MTEyOA==.html

请加小助手微信：QOS-Official

「　扫码加小助手好友　」