

WHITE PAPER



QOS项目白皮书

下一代企业级应用社区

| 2018.07 |

Version 0.6

目录

INTRODUCTION

前 言	1
1 QOS内涵	3
2 QOS整体架构	4
2.1 QOS双层链架构	4
2.2 QOS双层代币体系	8
2.3 QOS双层挖矿机制	12
2.4 开发者社区生态	12
3 QOS技术基础设施	14
3.1 共识体系	14
3.2 钱包体系	19
3.3 统一身份认证	20
3.4 IPFS文件系统	22
3.5 QOS公链区块链浏览器	22
3.6 QOS as a Service	23
3.7 小结	24

4	QOS公链的愿景：下一代企业级应用社区	25
4.1	用户社区	25
4.2	QOS生态业务场景	27
4.3	QOS的经济模型	30
5	团队和代币发行计划	33
5.1	项目路线图	33
5.2	QOS公链代币发行计划	33
5.3	核心团队	35
5.4	顾问及合作伙伴	36
5.5	联系方式及社群	38

前言

INTRODUCTION

从2015年接触区块链，我们一直在思考、研究、尝试如何与我们的现实业务相结合，如何服务实体经济。如同20多年前互联网开始影响和颠覆传统经济一样，我们坚定的认为，以区块链为代表的新技术、新模式将再一次改造传统经济，改变原有的利益格局，进而充分释放社会的创新力和协作热情。

我们团队和我们的合作伙伴具有高标准、合规的管理水平，庞大的用户群基础，完整成熟的产业生态资源，以及强大的技术创新能力。我们决定顺势而为，拥抱通证经济，着力打造“下一代企业级应用社区”。**通过底层公链把传统公司化行为转换成社区行为；通过通证把中心化激励体系变成社区自激励体系。**

企业级应用在“大众创业，万众创新”的政策背景和人口红利消失、办公成本不断提高的市场环境中，需求井喷式增长，但由于所处行业、市场环境、商业模式千差万别，往往呈现出业务流程复杂、跨业务主体数据交互频繁、服务质量要求极高的特征。经过我们的调研，**目前没有一套完整、行之有效、能够真正在线下生活场景落地的区块链底层公链，能够支撑广泛的企业级应用、大规模的分布式文件存取、统一的身份认证体系等需求。**

QOS通过打造基于公链与联盟链混合的**底层操作系统、统一身份认证体系、自激励的双层代币协议、超级节点+交易挖矿的双层挖矿机制、分布式文件系统、联通开发者和用户的互动社区**，支撑包括消费、传统金融、金融科技、新媒体等在内的海量用户级别的原生社区，并允许各类服务商在协议框架下便捷的发布新应用，逐步通过数据交易实现社区公民价值最大化。

我们确信QOS公链能够**填补比特币和以太坊等主流公链的市场缺位**，
率先将区块链技术应用于实体经济中，达到商用级服务水平，**触达和服务与
现有币圈完全不同的社区群体**。QOS公链致力成为全球覆盖人口最多的区块
链应用社区，实现广泛的社会价值、经济价值。

基金会主席：



2018.7.20

1 QOS内涵



QOS是乾元社区的底层操作系统。“chain”中文谐音“乾”。“乾元”出自《易经》，“大哉乾元，万物资始，乃统天”。大，蓬勃盛大；乾元，意指乾元之气；资，资源；始，创始化生；统，统贯；天，即天道。概括起来，即指蓬勃盛大的乾元之气是万物创始化生的动力资源，这种强劲有力、生生不息的动力资源统贯于整个天道运行过程之中。QOS作为下一代企业级应用平台，其生生不息的产业生态和创新应用将贯穿于整个区块链时代之中。故取“乾”首字母“Q”。

QOS亦代指Quality of Service 服务质量，通过构建新的社区基础设施，QOS希望提供质量一流、生态透明、过程可控的社区服务。

2 QOS整体架构

QOS系统引入一种新的区块链架构，探寻安全，性能与成本三者之间的平衡，解决日益丰富的应用对区块链技术和稳定可扩展的运行环境的需求，降低整体交易成本，满足商业环境中多变的交易需求，以创新的激励机制保证整个系统稳定公平的运行。QOS系统配套实现Service mesh架构，使开发者天然以cloud native的方式工作，方便开发者专注于业务实现本身。

2.1 QOS双层链架构

现有区块链技术在单链架构下存在性能、容量、隔离性、扩展上的瓶颈。区块链数据存储采用链式存储导致无法水平扩展，而共识机制同步模型导致无法高效处理交易，另外一些业务需要数据高度隔离也与单链架构冲突。

采用多链方式来满足可扩展性和隔离性，每个区块链维护了自己独立的价值体系。但是不同价值体系也有价值交换需求，这就需要区块链间的互操作性。

我们提出一种架构(QOS Chain)，通过双层的区块链体系和相关协议、底层接口设计，能够实用性地支持商业级别的可伸缩性和隐私保护。

2.1.1 概述

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和运营体系、文件系统体系等服务。

业务链可以采用联盟链或私有链方式通过实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——QOS星座协议，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。

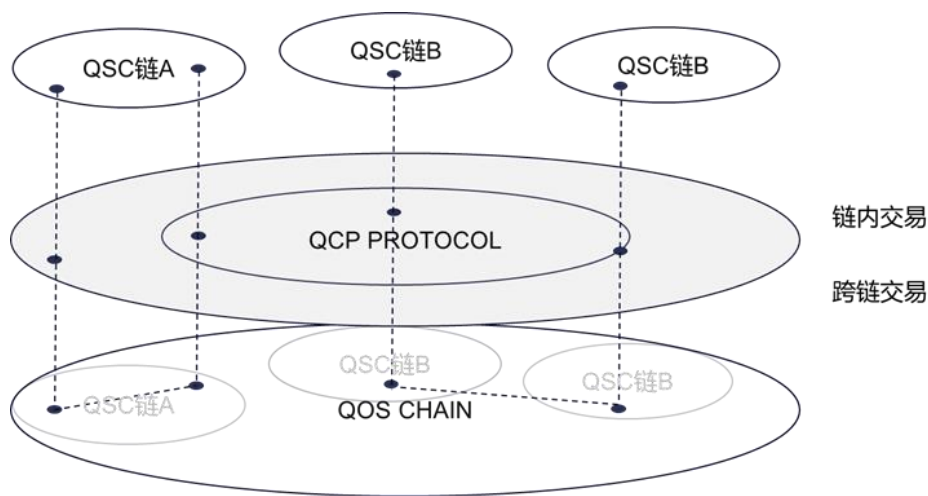


图2.1 QOS双层链架构

2.2.2 双链架构

1、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、业务服务提供者、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基础验证人必须要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 跨链协议

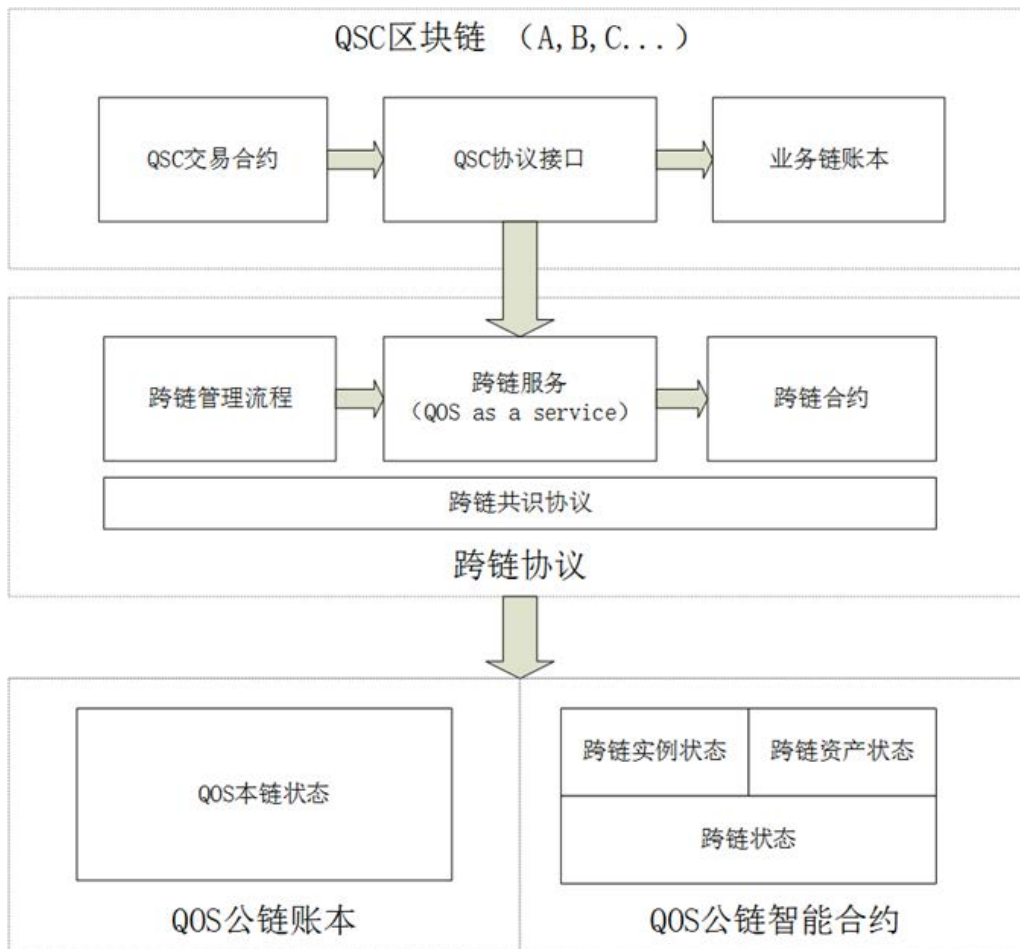


图2.2 QOS双链通信机制

● QOS基础链

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，以及跨链合约封装为gRPC服务以简化业务链调用跨链交易。

● 业务链

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。

- 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。

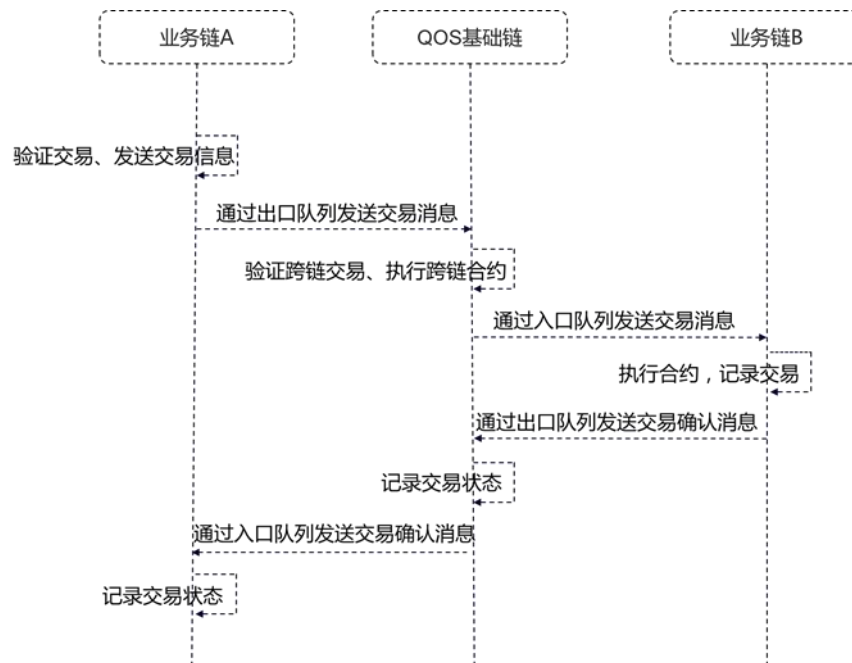


图2.3 QOS跨链交互的时序示意

2.2 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。

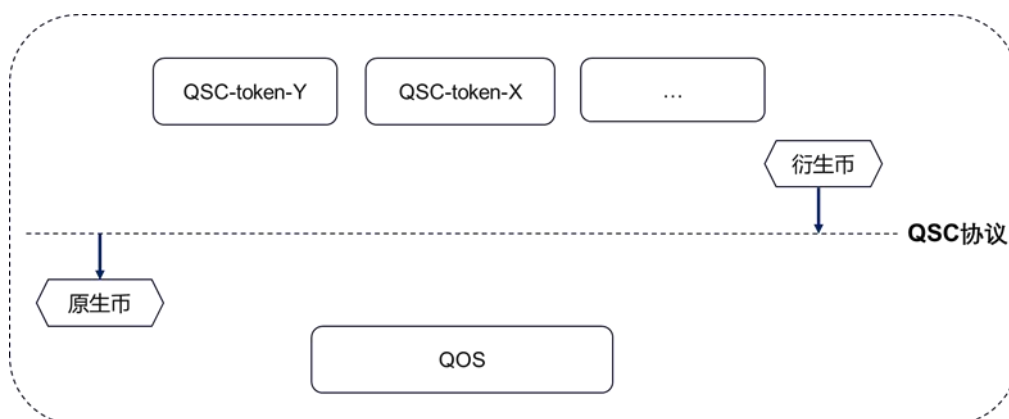


图2.4 QOS双层代币示意图

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QPC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代币具有更好的流通性。

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：

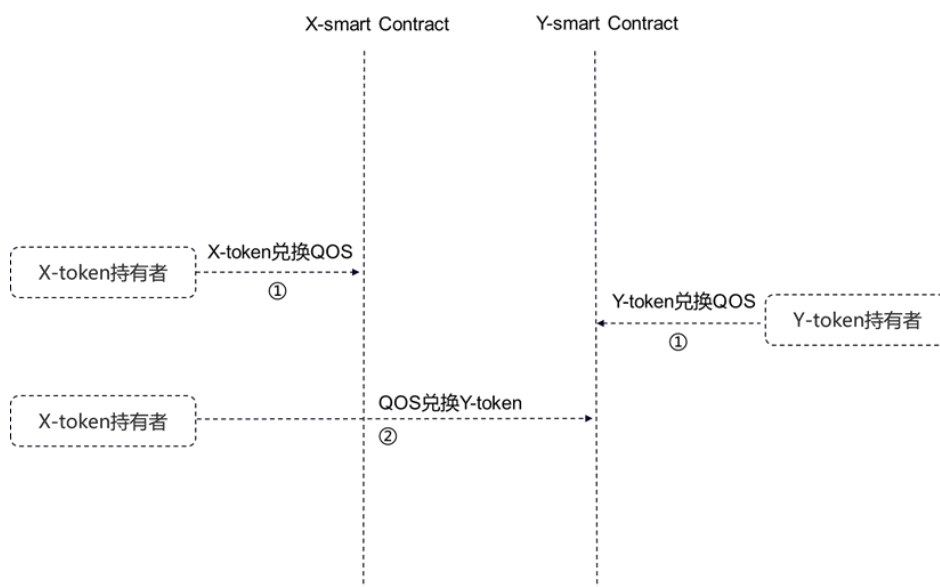


图2.5 QSC协议代币之间兑换流程

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：

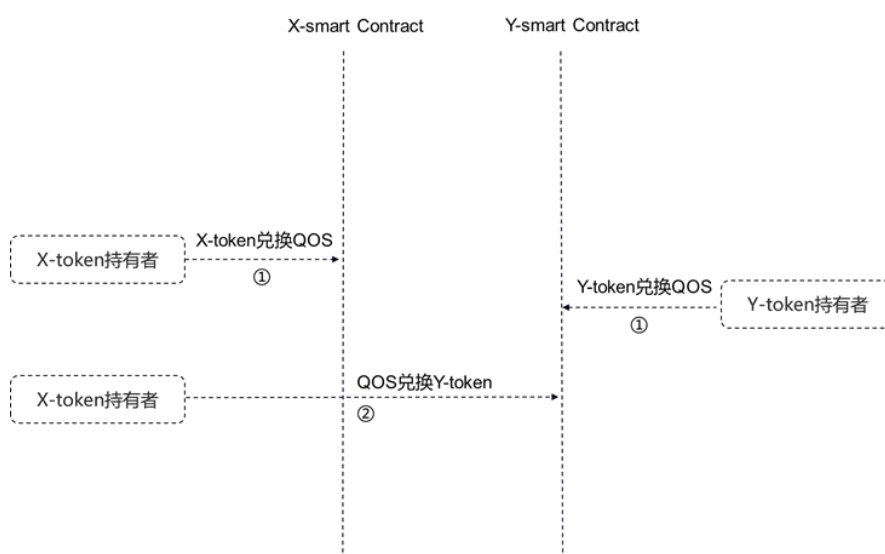


图2.6 QSC协议代币与QOS公链外代币交易流程

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达到3秒。

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

$$\mu = \text{取整}\left(\frac{\text{当前时间} - \text{QOSChain初始时间}}{T}\right)$$

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	1.59375
新区块奖励 QOS数量 (枚)	60.64	30.32	15.16	7.58	3.79	3.79

2.3 QOS双层挖矿机制

与双层代币模型相对应，QOS生态建立双层挖矿机制，在QOS公链由21个超级节点竞争挖矿。在各个场景主张“价值交换即挖矿”，具体而言，可以是“交易即挖矿”、“借贷即挖矿”等不同模式。

详见4.3QOS的经济模型。

2.4 开发者社区生态

QOS基金会发起的QOS开发者社区，为开发者搭建从创新到商业应用到桥梁。QOS开发者社区是一个QOS开发爱好者的聚集地，QOS开发者

社区将给所有的开发者提供一个任何人都可以参与贡献的开源社区。社区的宗旨是打造完善、自由、民主的公链生态平台。QOS 基金会发起的开源项目托管于 GitHub ,每个开源项目都会发布一个任务列表 TODO ,社区开发者根据自己的兴趣爱好可以选择项目贡献代码并获取相关的激励。

QOS具备完整的生态：

- 1、用户基于QOS主链钱包，使用系统的场景服务
- 2、VIP合作伙伴加入记账体系，拥有挖矿资格
- 3、开发者基于QSC协议发行自己的加密数字货币，币通过QCP protocol协议实现跨链交易
- 4、开发者基于某一QSC代币发起一个项目，创建自治组织
- 5、开发者基于社区生态开发新项目

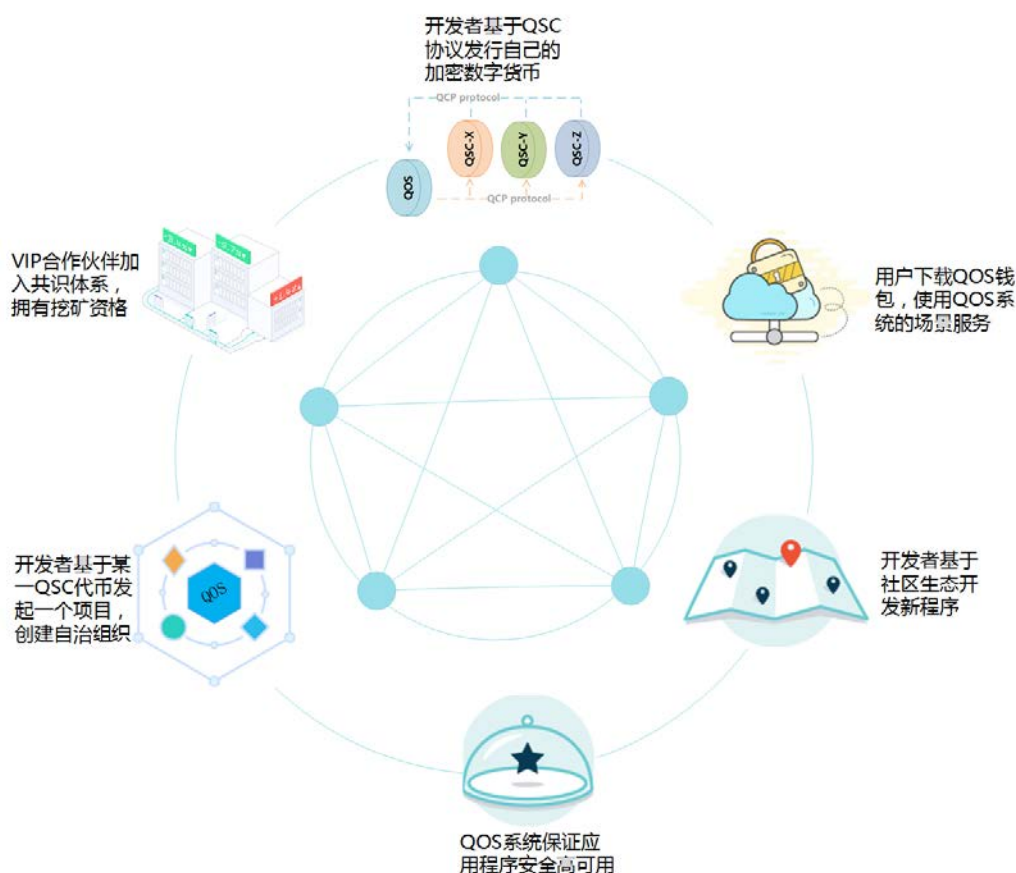


图2.7 QOS开发者社区

3 QOS技术基础设施

QOS希望通过引入一种新的区块链架构，探寻安全，性能与成本三者之间的平衡，解决日益丰富的应用对区块链技术和稳定可扩展的运行环境的需求，降低整体交易成本，满足商业环境中多变的交易需求。

3.1 共识体系

3.1.1 技术痛点

- 性能与成本

区块链发展到今天，交易的性能已经是很突出的问题，尤其是作为基础服务的公链，将面对大量的应用，复杂的智能合约以及超大规模的用户。同时，现代社会出现的多种商业模式以及丰富的应用场景，对降低交易成本，以及交易成本的可配置性提出了更多要求。高昂的交易成本和简单粗暴的矿工费模式，会阻碍基于区块链的应用，同时阻碍链自身的发展。

因此交易的性能与成本虽不是区块链技术体系的根本目标，但已经是不可忽视的需求。

- 稳定性与扩展性

智能合约需要稳定的运行以提供服务。随着合约用户规模的增大，合约也面临着扩容的需要。同时在这基础之上，稳定性和扩展性也应当包括对合约错误的纠正与合约功能的扩展，以不断提高合约的稳定性，并且拓展合约所能提供的服务。因此，智能合约不仅需要保障扩容运行等各种技术手段，也需要升级合约等维护性功能。

- 一致性与安全

作为基础服务的公链，需要保证链上数据的一致性，防止各种威胁，以

保证记录数据的不可篡改，从而保证数据的安全。并且区块链的安全，不仅仅指来自恶意外来者的攻击，也包括避免合法参与者造成的错误或故障，以及潜在的可能导致链自身被单方面控制的危险。

3.1.2 解决方式

1、性能与成本

安全与性能从某种角度讲是互斥的，因为出于安全目的，可能需要大量的验证计算和反复的交互通信。因此为了能够在两方面找到平衡，引入双链架构，上层联盟链或私有链用于业务支撑，可以并发的处理大量异构业务，以提供高性能的服务为目标。底层为公链，核心目标是保证数据安全和交易可验证，防止篡改。

降低整体使用成本，让使用者可免费使用（上层应用中的绝大部分状态变更不需要向矿工直接付费），会向服务提供者（智能合约发布者）收取费用，这样合约发布者可以决定不向使用者收费，也可以在智能合约中开发定制的付费模式，从而实现丰富的应用模式。

2、稳定性与扩展性

为了提供给智能合约稳定性与扩展性，采用容器技术，以及相应的管理、监控等技术，提供实时的数据分析，以提供智能合约稳定和可扩展的运行环境。允许升级合约，保证合约的稳定运行和功能拓展。

3、一致性与安全

区块链的数据一致性以及安全依赖于共识算法，下面就共识算法进行说明。

3.1.3 区块链的潜在缺陷

- POW

浪费过多非必要的资源，这会直接导致链上交易成本的不断提高。并且基于算力的共识算法是会受到相关资源直接影响的算法，从现实情况看，很难限制和避免资源的过度集中。

- POS

虽然一定程度避免了资源的浪费，但由于仍然需要全网确认区块，性能仍有一定瓶颈。尤其目前仍然存在诸多缺陷，还不能有效的避免多种经典攻击问题。

- DPOS

由于优化了确认区块的方法提高了性能，但仍有一些被攻击的隐患，从现实情况看，这些隐患可以肯定会被黑客反复尝试攻击：

- > 无利害关系问题（Nothing at Stake Problem）
- > 长距离攻击（Long-Range Attack）
- > 贿赂攻击（Bribe Attack）
- > 持币时间累计攻击（Coin Age Accumulation Attack）
- > 预计算攻击（Precomputing Attack）

由于以上原因，基于DPOS设计基础共识算法。

3.1.4 QOS公链共识算法设计

借鉴以往的区块链项目经验，预选共识节点（共识参与者）不宜过少（11个左右），过多也会有一定资源浪费（31个以上）。因此折中竞争选择出21个超级节点负责共识和生产区块。

在一个共识周期中，所有超级节点都有公平（不等于相等）的机会生产

区块。所有超级节点应在共识周期内保持100%在线，如果不在线，则失去本次共识周期内的投票机会和被选举机会。如果超级节点在共识周期中出现任何被认为反常的操作，都有可能丢失投票和被选举的机会，甚至可能被全体有效超级节点联合投票踢出。

共识算法同时需要关注解决前面所述的问题。

- 无利害关系问题

共识将明确禁止多重投票，以避免“无利害关系问题”，被检测到多重投票的超级节点将被认为是故障节点失去本次共识周期的投票和被选举机会。

- 长距离攻击

限制接受的分叉节点数量，以保证链的一致性。

- 贿赂攻击

由于采用使用者免费的策略，因此应该能够避免“贿赂攻击”。

- 持币时间累计攻击

为了更公平而引入“时间”（不可累计的资源）作为计算参数之一，极易引起“持币时间累计攻击”。因此引入的衡量参数不应是“时间”，共识引入“时效”作为计算参数之一。“时效”在有效时间内有效，过期会失效。将大大降低可能的攻击风险和损失。

- 预计算攻击

为了降低预计算攻击的可预计性，引入全节点交易总量作为计算参数，由各个共识节点报告自身在共识周期内的交易量，合计为一个总量参数，即使存在恶意节点伪造报告的交易量也很难操纵整个网络。

总结，以DPOS为基础实现定制的POS共识算法。在共识中引入“时效”和“交易量”两个重要的参数。“时效”可以限制权利的有效期，从而

降低作恶的可能性。“交易量”则是诚实者几乎不用付出的成本，而潜在作恶者需要付出巨大的成本。“交易量”参数将作为不是惩罚的“惩罚”约束潜在的作恶者。

3.1.5 交易的确认与区块的生成

多笔交易会打包生成一个区块。并提交给共识周期中选举出的代理超级节点确认。

每个区块生成块的阈值预设为达到3秒，正常情况下，确保一个交易被计入到链中需要超过2/3的拥有权益的超级节点确认该交易。以21个超级节点为例，即需要15个节点。参考正常的交易业务系统，用户友好的体验需要在秒级给出反馈结果。交易确认可以并发执行，因此正常的平均入块时间可在1秒以内。在异常情况下（软件，系统或硬件，网络异常，以及普通的恶意攻击），为了确认交易被正常的计入链中需要15个超级节点确认，因此异常情况下的交易确认平均在15秒以内（15倍单个入块时间）。同时由于DPOS 共识是代理权益证明方式，由推选出的代理超级节点确认交易，合理情况下，代理超级节点推选数预设为7，因此理论上异常情况下的交易确认平均时间可在7秒以内。

监测系统会监测链中各个模块或子系统，以保证整个链的稳定服务。同时会严格监测超级节点异常，或交易确认异常，如果出现异常，首先会向相关用户和负责人发布报警信息，如果异常符合预设情况，则会根据不同的设置临时禁止超级节点的投票和被选举权，或者通知所有有效超级节点发起一轮投票，判定是否异常的超级节点需要被踢出。

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：

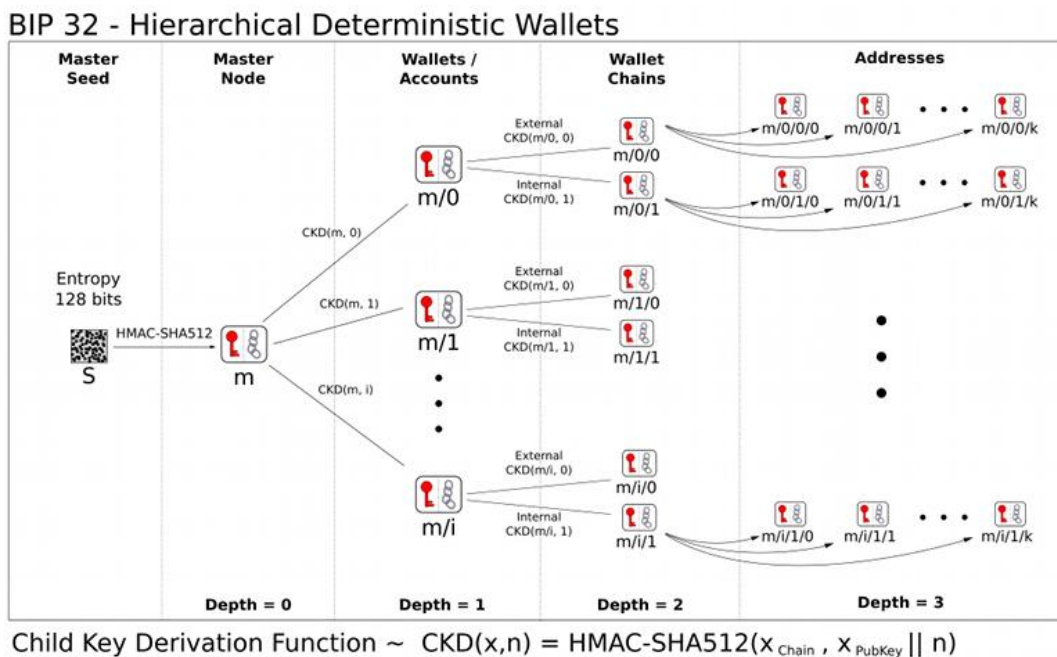


图3.1 BIP32协议原理

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。

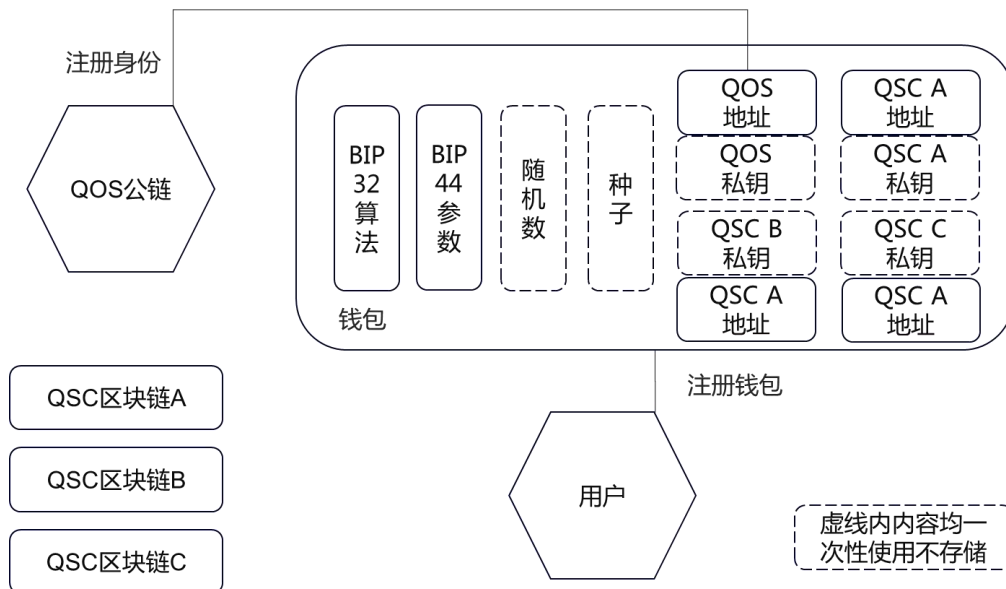


图3.2 QOS公链用户钱包整体结构图

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：

1、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。

2、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。

3、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。

4、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。

5、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。

6、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。



图3.3 广义身份

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。

3.4 IPFS文件系统

QOS公链计划自建IPFS节点作为数据存储和分发基础设施，使得在QOS公链里所有的数据都流动起来，解决数据孤岛的问题。信息的存储、定位和移动会被重新设计，QOS公链里所有设备的存储被统一管理起来，从这个层面理解，QOS是一个网络操作系统，在这个系统里，终端节点只有一个小的启动系统，当系统启动的时候，所有数据将从网络下载，同时能保证终端节点快速下载和使用数据。

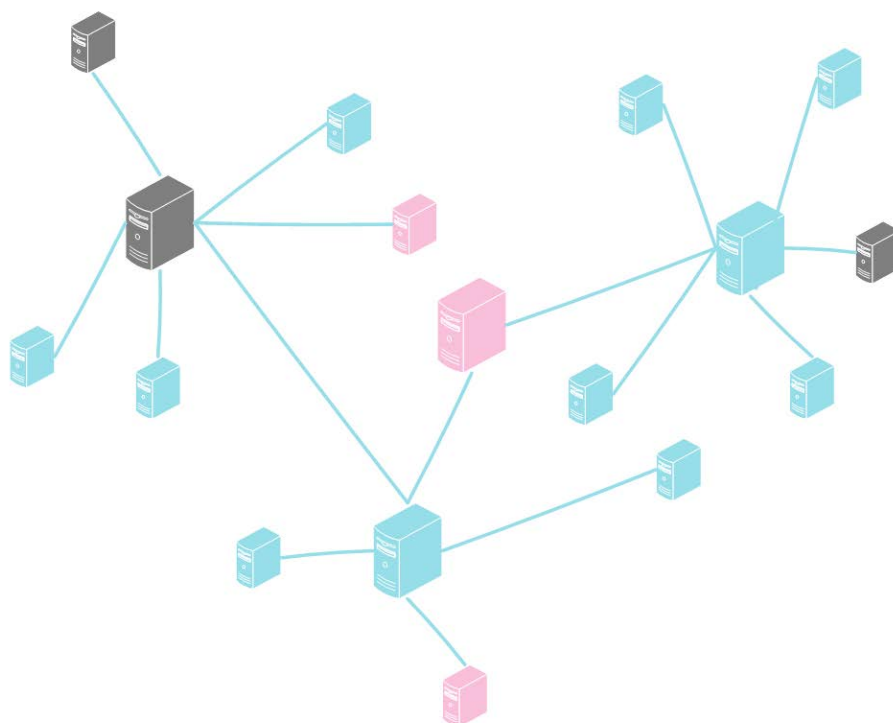


图3.4 QOS公链文件系统

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qoschain.info。QOS开发者API和区块链浏览器的架构如下图：

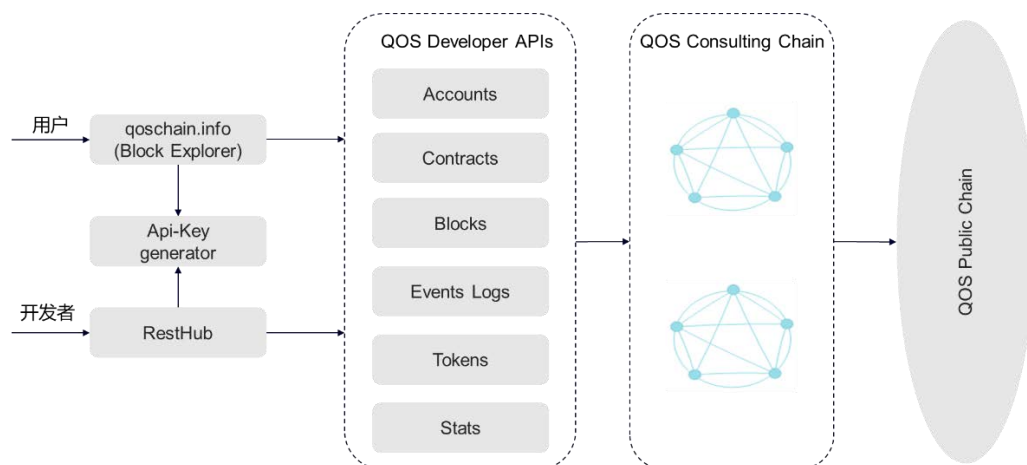


图3.5 QOS公链区块链浏览器

3.6 QOS as a Service

基于容器云、资源调度技术，QOS配套实现Service mesh架构，使开发者天然以cloud native的方式工作，方便开发者专注于业务本身。QOS的Service mesh架构松耦合的部署在应用程序代码旁边，以网络代理的“数据平面”和用于与这些代理交互的“控制平面”的形式，解决程序运行时的问题，较好的支持系统的异构，不局限于某种语言或协议。QOS as a Service的架构如下图：

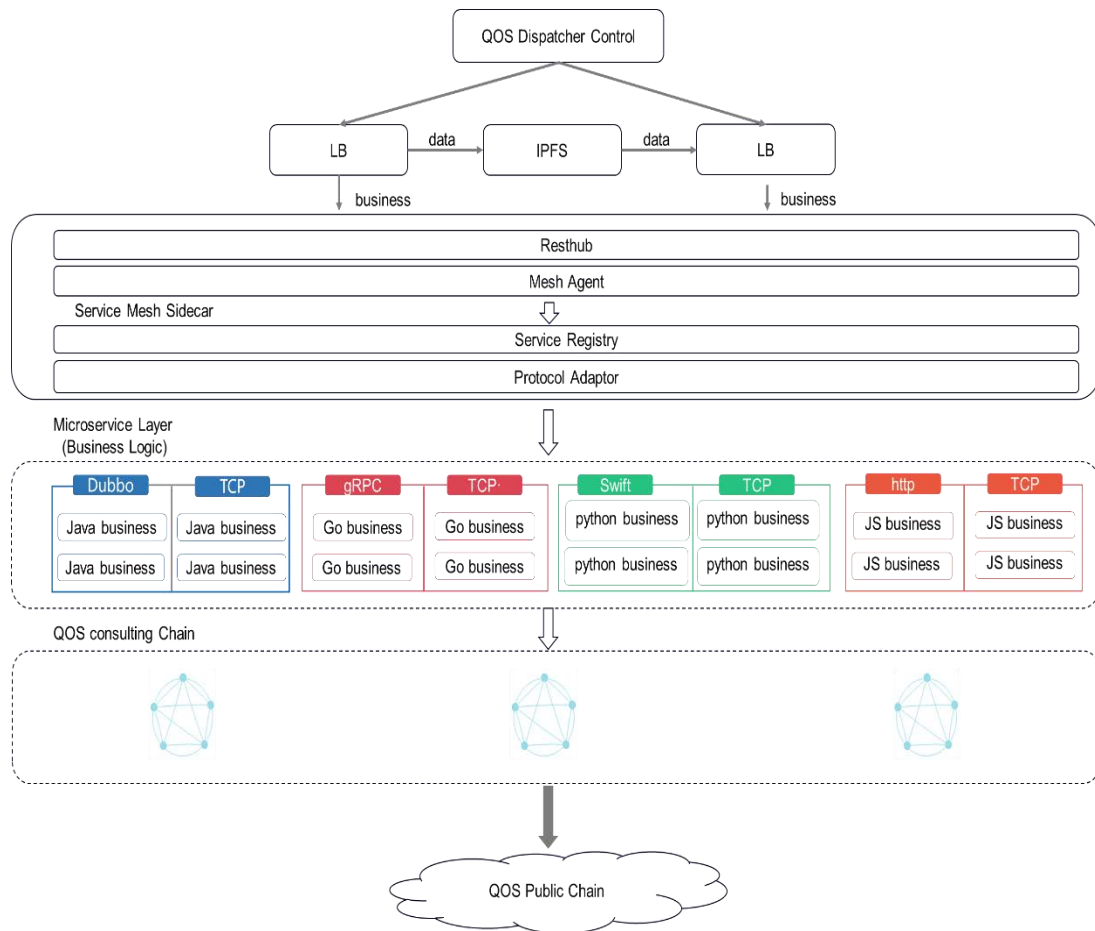


图3.6 QOS as a Service

3.7 小结

QOS公链采用双层链架构实现性能和容量的扩展,同时实现QCP跨链协议,把业务逻辑和底层公链分而治之,在提升交易性能的同时让开发者更容易实现自己的分布式区块链应用。安全去中心化的资产托管,方便用户基于钱包实现去中心化交易。

QOS公链系统是基于实践考验的概念来设计的,代表着区块链技术社区的实践落地。QOS公链和QSC协议提供的生态,是可扩展区块链社区的一部分,为开发者提供完整的区块链场景。

4 QOS公链的愿景：下一代企业级应用社区

QOS公链作为下一代企业级应用社区，生态将包含消费、支付、金融、媒体、生活服务、社交等一系列场景服务商，并开放接口给社区，不断的扩展应用领域，发动社区完善公链钱包、去中心化交易所、数据服务等配套技术设施和相关产业内容，以逐步完善生态。

4.1 用户社区

QOS社区的建设作为一个有步骤的系列运营行为，离不开社区公民的活跃和贡献，QOS公链首先应用于战略合作伙伴——**钱包星云**。

钱包星云通过“**数字资产+数字通兑积分**”打通QOS社区第一批企业应用的账户系统，包括钱包生活、钱包金融、卡惠、停车钱包等。在钱包星云体系内，各企业应用场景通过QOS公链形成统一的链上身份，对接已有的通用积分体系，并可依据QSC协议自行发布数字资产。

目前钱包生活活跃商户达到**40万**，触及C端用户可达**5000万**规模。钱包金融拥有高素质活跃用户**百万**以上，卡惠总用户量**500万**左右，停车钱包服务**1000万**车主。这些用户将通过钱包星云的服务在QOS公链上形成统一的链上数字身份。同时，钱包星云亦向所有愿意加入QOS公链的分布式应用开放，并维持链上统一数字身份。

钱包星云在完成统一数字身份之后，将帮助用户把分布在各个应用场景中的各种权益转化为数字资产。在这一过程中，也将帮助各场景自行设计权益和数字资产之间的转化方式，激励各场景发挥自身优势，根据各自对用户服务的理解，创造性的发行数字资产。钱包星云本身也将进行示范性的数字资产发行，形成各场景应用的互动，并通过数字资产的多样化，提升整个场

景的获客能力，培养用户使用数字资产的习惯，享受数字资产的各种权益。

在发行企业级场景数字资产的同时。QOS社区将在钱包星云的基础上进一步发展，利用独特的新媒体传播方式，打卡、邀请、空投激励等方式使得QOS社区的每一个用户都逐步拥有高等级数字资产。并在用户使用数字资产的习惯养成基础之上，促进高等级数字资产的流通，形成活跃的社区氛围。QOS社区的公民享有全部的自治权和公民权，将通过数字资产分享体系建立参与热情，打造形成共识的“劳动者社群”，团结社群的力量，共同实现共享的经济体，源源不断的为整个QOS生态导流。

QOS生态已经有非常成熟的支付公司、商业银行、互联网金融、新媒体公司作为合作场景服务商加入，300个城市超过40万本地商户、1000多个停车场的交易场景将建立在QOS平台之上，合计月交易流水超过60亿元，交易笔数超过3000万笔，平台将触达5000万以上的交易用户，每月将产生超过20亿元的借贷需求。未来会不断孵化、接纳例如出行、外卖、快递、社交服务商。

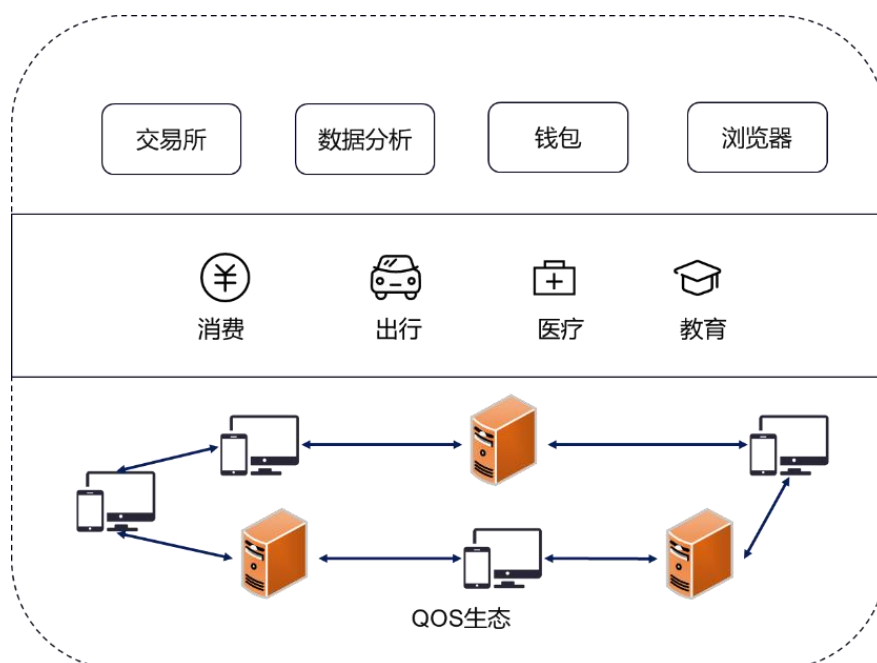


图4.1 QOS生态示意

4.2 QOS生态业务场景

4.2.1 消费（生态服务商：钱包生活、停车钱包等）

中国超过85%的零售交易发生在线下，是一个规模33万亿的交易市场，仅有的线下数据散落在中小商户的管理系统、个人银行账户、第三方服务商手中，公民身份信息一方面得不到存储和利用，另一方面也导致“数据贩子”横行，隐私被不断侵犯。

如今大量数字货币的流行是对区块链技术的肯定，而支付才是数字货币的本质，但现存数字货币大部分只能应用于线上，线下场景分散且没有机构能够整合，在用户持有多多种数字货币的情况下，如何能够将数字货币应用到广阔的线下支付蓝海市场是亟需解决的问题。

因此，QOS社区将第一个应用场景选择为线下消费，而合作的支付服务商也意识到传统集中式的交易服务所隐含的数据风险、隐私风险，正在积极推动商户、用户、场景向区块链产业转型。首个生态合作方——钱包生活定位本地消费买单平台，平台向本地中小商户部署智能POS机/二维码支付、提供智“惠”营销服务，为C端用户提供“闪付+白条”功能，目前已全面覆盖300个城市，超过40万家美食、休闲娱乐、运动健身、生活服务、商业超市、丽人等商户，月交易流水超过60亿元，交易笔数超过3000万笔，累计交易用户超过1000万人。

另一个支付生态服务商——停车钱包从停车服务切入，为车主、停车场、广告主（本地中小商户）提供服务，通过提供软硬件一体的停车场管理系统为车主提供无感停车支付服务，并根据位置数据为广告主推送潜在客户，项目已经深度覆盖23个城市，运营1000家停车场30多万个车位，服务车主超过1000万人。

4.2.2 金融信贷（生态服务商：钱包金融、钱包好车、长治银行等）

金融信贷的过程本质是一种识别用户身份并为其定价的过程，传统金融实际是垄断资源（牌照、数据、低成本资金...）的变现，催生大量资金掮客，广大中小企业和没有信用记录的个人借款利率畸高，享受不到应有的服务。近几年互金行业的高速发展让我们看到“弱势群体”的“金融饥渴”。中国的借贷市场仍极其广阔，社会融资规模存量156万亿，其中网络信贷规模2.2万亿元，我们认为区块链将从多个方面改变传统金融服务：

1、区块链能够保障资金用途和交易一致性：传统金融虽然有合同约定，但筹资人借到资金后，实际上拥有自主使用权，很难防止挪用，由此造成出资人风险。传统金融对于资金用途和交易一致性没有有效解决方案，只能退而求其次将注意力完全放在还款能力、抵押物和意愿上，间接承认资金用途的不可控。在区块链、智能合约和数字货币时代，完全可以通过联合签名机制来有效监控资金用途，要求数字货币的支付必须要多方同时签名认可才能完成，筹资人在收到数字货币后并没有完全自主使用权，从而有效防范了挪用风险。

2、由于身份信息全面、安全、可控，区块链时代的信贷将逐步过渡到P2P信贷时代，金融服务商将转化成为信用信息服务商，有借款需求与有理财需求的个体利用专业的信用数据服务进行点对点信贷、投资。

基于以上观点，QOS高度重视金融市场的发展，在社区成立初期就与不同类型的金融机构达成了合作意向，共同推进下一代金融科技的演进。

● 商业银行

商业银行是中国金融信贷的主力军，中国人民银行征信中心的个人信用报告更是在前区块链时代公民信用的最权威体现。社区建立初期，有商业银行加入将会极大的促进公民信用体系的建设。长治银行作为积极拥抱新兴产

业的地方性股份制银行，将是QOS社区成立初期的重要金融信贷服务提供方。

● P2P

网络借贷信息平台凭借着投资金额门槛低、收益率较高、期限较为灵活的优势，已经成为C端用户的重要理财渠道之一，随着网贷平台信息中介的身份被确认，并逐渐接入银行存管，安全性不断提升，但服务器集中部署，安全隐患仍在存在，实际操作中容易被不法分子攻击，直接威胁用户数据隐私、资金安全。

通过QOS搭建的区块链平台，在上面运行互联网投资借贷应用，并配合相应的智能合约开发与执行环境、底层分布式账本，出资人将资金直接转移给筹资人，无需存管账户，也没有沉淀资金风险。

QOS在理财领域的首家战略合作伙伴是一家全国领先的网络借贷平台，该平台稳健运营超过5年，累计交易额超过400亿元，投资用户超过50万人。

● 汽车金融

汽车金融作为迅速发展的金融形态，与无固定使用场景的信贷资产不同，车主在享受金融服务的过程中还将留存一系列的车辆、出行、消费信息，对于构建完整的社区生态具有重要意义。

QOS社区的首个汽车金融场景服务商钱包好车是中国车抵贷规模排名第2的汽车金融服务提供商，在全国近300个城市有线下服务网点，月放款金额近10亿元。

4.2.3 媒体（生态服务商：星红安等）

公民在媒体平台上的有效浏览、评论、转发、活跃度都代表着自身对于社区的贡献度，也体现着独一无二的爱好、品味信息，在平台建立初期就应该有相应的服务商提供服务。

目前大多区块链项目在媒体方向的应用是互联网广告领域，原因在于互联网广告的IT基础设施完善、竞争更加市场化。这种业务模式存在两点缺陷：首先，单纯互联网广告平台使用户身份的内涵被不恰当的缩小，仅仅依托于用户在互联网上的浏览记录进行分析、变现价值并不高。其次，广播电视由于其庞大的用户基数、强大的终端影响力，在人们的生活和广告主的营销渠道中都扮演着重要的角色，但由于基础设施尚未健全，这部分没有被现有模式纳入进来。

QOS社区将在电视广播媒体领域进行应用，搭建一个国内领先的以电视屏为入口，整合三屏合一的数据服务平台。目前平台已集合全国超过20个省级网络运营商的家庭收视行为数据以及DPI上网流量数据，覆盖用户超过7000万户，为北京、天津、上海、重庆等15个广电网络运营商提供数据采集和分析服务，旗下传媒公司已取得全国37个城市数字电视广告代理资格，业务覆盖23个省、500多个城市，是国内规模最大、覆盖面最广的数字电视广告联播网。

QOS社区未来也会吸纳中国最大的三四线城市新媒体运营平台，该平台整合了800个县域地市的本地新媒体，为新媒体赋能，提供商户管理、会员管理、营销支持、团购等服务，是中国最大的县域新媒体服务商之一，平台月UV超过1000万，超过500万用户在平台上产生交易。

4.3 QOS的经济模型

QOS将建立双层代币模型，分别为QOS公链代币和QSC协议代币。QOS是公链代币，是社区通用货币，各消费、金融场景都用QOS代币作为价值储藏手段和支付手段。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。QSC协议代币为各场景运营商根据自身体系的需求自主发

行，持有者为各自场景的权益最终所有人，享有场景内的收益分享权利。

与双层代币模型相对应，QOS公链建立双层挖矿机制，在底层公链由21个超级节点竞争挖矿，在各个场景主张“价值交换即挖矿”，具体而言，可以是“交易即挖矿”、“借贷即挖矿”等不同模式。

1、公链超级节点挖矿机制：每笔交易的发起方都需要另付一定量的QOS公链代币作为矿工的打包费用，打包费用的多少根据交易金额、复杂度、打包上链及时性而有所不同，平台会给出相应参考值。

2、具体应用场景的“价值交换即挖矿”机制：以消费场景举例，该运营商发行QSC1作为其场景权益代表。该场景内的价值交换体现为消费，因此消费就是挖矿行为，支付、收款双方都将获得相应的QSC1挖矿奖励，即各获得价值等同于支付手续费一半金额的QSC1，挖矿结算周期为天，QSC1与QOS的兑换比例将按照该结算周期内的平均汇率结算。每笔支付，支付方将支付一定量的QOS作为支付手续费，该手续费将分成2部分，其中80%分配给QSC1持有者，20%用于QSC1社区开发及运营，收益分配结算周期同样为天。

场景运营平台可以预留一部分QSC1作为团队激励、运营费用，但预留部分必须随着体系内的价值交换行为同步解冻。

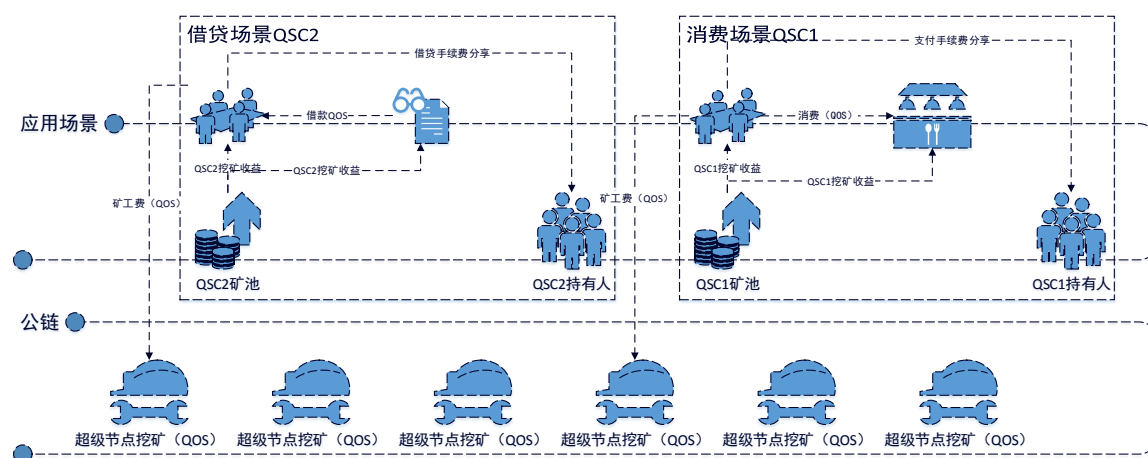


图4.2 QOS双层代币模型

QOS倡导“价值交换即挖矿”，价值交换既可以是有形的商品买卖、服务消费、金融借贷，也可以是无形的关注度、浏览量等等，只要有广告主、广告公司或其他任何机构、个人愿意为用户的关注、浏览支付费用，QOS就认可其为价值交换，就将是一种挖矿行为。

QOS早期阶段会与代币交易所合作为用户社区提供完善的数字资产管理服务，具体做法分为两步：

1、用户转化：QOS主网上线之前，代币为ERC20兼容代币，为了保证所有的社区用户都能低门槛的享受到数字资产服务，首先会将QOS的海量基础用户导流到交易所，建立完整的数字资产钱包体系，将传统社区用户转化为基于区块链的QOS社区用户。

2、用户激活：与各大场景运营商合作进行QOS的空投，定制签到、拉新、消费、理财等一系列运营活动，对QOS社区内的用户进行数字化营销，培养QOS社区用户的数字资产使用习惯。

QOS主网上线后即采取“交易即挖矿”、“借贷即挖矿”等模式进行社区回馈。

5 团队和代币发行计划

5.1 项目路线图

表5.1 项目路线

2018Q2	项目筹备
2018Q3	完成私募；白皮书发布；战略合作伙伴签约；核心社区建设
2018Q4	公有链测试环境与QOS钱包发布；QOS生态基金成立
2019Q1	公有链配套服务工具开发；持续应用场景的投资和合作
2019Q2	公有链生产环境发布

5.2 QOS公链代币发行计划

QOS公链代币全球定量发行100亿枚，其中51%由挖矿产生。

具体的分配方式如下：

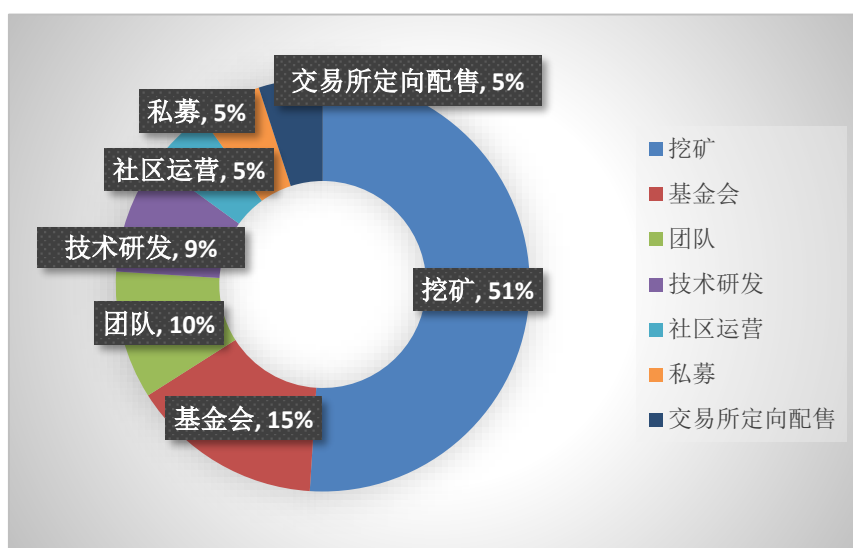


图5.1 QOS公链代币分配方式

其中团队持有代币将锁定12个月，随后将在2年内按月等比例进行解禁。

QOS计划募集融资50,000枚ETH，其中私募融资25,000枚，交易所定向配售25,000枚。募集时间表为：

表5.2 QOS公链代币募集时间表

轮次	额度	截止时间	价格ETH:QOS
募集	50,000ETH	2018.8.4	1:20000

QOS社区将在新加坡成立基金会，作为社区治理的主体，全面负责管理QOS技术研发和商业应用落地以及合规审计相关工作，宣传推广QOS品牌。

5.3 核心团队



张 哲

基金会主席

前奥马电器（002668）副总经理，战略发展部总经理，区块链业务负责人，钱包投资管理合伙人，负责上市公司战略和投资业务。

汉世纪创投执行总裁，16年资本市场及创业投资经验，曾参与主导投资安硕信息（300380）、万得资讯（Wind）、通付盾等知名企业。



汪怡宁

曾任奥马电器（002668）投资总监，作为核心成员参与上市公司多支产业投资基金设立，主导多个金融科技项目投资，钱包集团体系资源协调整合。

北京师范大学本科，中国社会科学院研究生院硕士。



李 杰

曾任奥马电器（002668）架构负责人，曾参与中国人民银行法定数字货币原型设计工作。阿里巴巴工作6年，担任资深开发、架构师职位。

13年开发架构经验，擅长大型互联网系统架构、技术管理。



周海京

安全专家，作为核心成员参与中国第一款通过CC EAL4+认证的国产安全芯片项目。主导钱包集团支付清算协会数字货币重点研究课题以及多个区块链金融落地项目。

清华大学自动化系本科、硕士、博士。



栾 悦

曾任钱包生活市场总监，曾任腾讯视频市场品牌负责人，负责腾讯视频整体品牌。曾任职于爱奇艺市场部、中国广播电视出版社等。行业记者出身，在互联网市场营销、品牌建设领域具有丰富工作经验。中国传媒大学硕士。

5.4 顾问及合作伙伴

5.4.1 顾问



赵国栋

奥马电器董事长 钱包金服创始人

中国第三方支付行业元老级创业家

中国支付清算协会常务理事

清华大学五道口金融学院EMBA

清华大学五道口金融学院互联网金融协会主席团成员



张 健

FCoin创始人 歌者资本合伙人

区块链行业早期开拓者，通证经济实践领军人物

《区块链：定义未来金融与经济新格局》作者

5.4.2 合作伙伴

场景生态



金融服务



技术服务



交易所



5.5 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

<http://weibo.com/u/6310001987>

微信群

QOS区块链微信群

请加小助手微信：QOS-Official

「 扫码加小助手好友 」

