# QbaoChain项目测评报告

**1、项目概述**

**QbaoChain-区块链服务提供者**

      QbaoChain作为定位于区块链服务提供者，为公司、组织等通过区块链技术落地其想法，致力于为不同商业场景提供整套解决方案。QbaoChain是一种联盟链(Consortium Blockchain)，拥有共有链不可企及的高效性能，兼具高安全、隐私等优点，同时还是支持多个行业的（金融、物联网、供应链、社交游戏等）部分去中心化的应用开发平台。参与到区块链系统中的每个节点都是经过许可的，未经许可的节点是不可以接入到系统中，区块链上的读写权限、参与记账权限按联盟规则来制定。

       其代币为QTC，将在QbaoChain上作为货币，为智能合约模块提供支持，并与许多应用兼容。它也将经由指定节点挖矿取得，QbaoChain为企业、开发者们免费提供平台货币用于商业场景探究和部分区中心应用开发。QbaoChain将利用智能合约在多个真实市场中应用到多个商业场景，比如：房地产市场、电子商务以及线上拍卖。相较于共有链平台如Ethereum等，QbaoChain具有TPS高达5000的极高性能，同时更加安全和隐私，直面解决共有链性能不高、数据不安全等痛点。

**2、基本信息**

     QbaoChain不仅完美实现了区块链不可篡改、不可伪造、不可抵赖、分布式、无需信任、点对点、集体维护等特点，QbaoChain从整体架构设计到节点编码开发；从共识算法到对象储存；从加密算法到广播策略；从性能调优到网络抖动QbaoChain都有巨大的创新与突破。因此，相对于原有公有链，QbaoChain具有更多明显优势。

**(1)功能强大**

采用BTC的UTXO账户模型，支持同时处理多个UTXO，因此具有良好的扩展性，可以实现并行事务并鼓励可伸缩性创新。同时，如果用户为每笔交易使用新地址，UTXO就可以提供强大的匿名功能，防止被追踪。除此之外，QbaoChain还支持强大的合约层，一个智能合约是一套以数字形式定义的约定，包括合约参与方可以在上面执行这些约定的协议。因为区块链的不可变和分布式特性，智能合约一旦被创建，这永远都无法改变，因此能够解决信任问题。

**(2)闪电般的交易速度**

BTC的交易速度为3笔每秒，ETH的交易速度是6.7笔每秒，IBM的超级账本理论峰值是200笔每秒，我们通过重新设计共识机制，分离共识步骤，先商量后打块，大幅度地提高了区块链网络的性能，在QbaoChain中，QbaoChain的交易速度可达5000笔每秒，随着未来网络带宽的升级，还将进一步提升交易速度。

**(3)更高的安全性**

联盟链上的信息不是所有条件的人都可以访问，只有该联盟链上的节点才能进行访问，因此能够提供高级别的安全性。不但具备了私有链的隐私性，还具备了公有链的去中心化思维，确保了链上数据的高度隐私，同时避免节点受到攻击的情况发生。

**(4)超轻量的存储**

BTC区块链需要巨大的存储空间达几十G空间，有些甚至更大，这需要节点提供专有大容量存储设备，在QbaoChain中，QbaoChain所需空间将缩小一百倍左右，甚至更小。因为它只需要存储区块链哈希树和关键检查点之后的数据，存储空间直接降到十几M甚至几M。

**(5)真正的私有钱包**

BTC/ETH一类的钱包必须要借助中心化的服务器，经常发生被盗事件，QbaoChain提供真正私有的去中心化钱包，钱包不再存放于第三方中心服务器上，而是直接访问区块链节点，更好的保护了钱包私钥，不再因为第三方信用问题、安全问题导致钱包丢失，实现了真正意义上无法被盗取的区块链私有钱包。

**3、代码评审**

**(1) 性能测试**

运行场景:

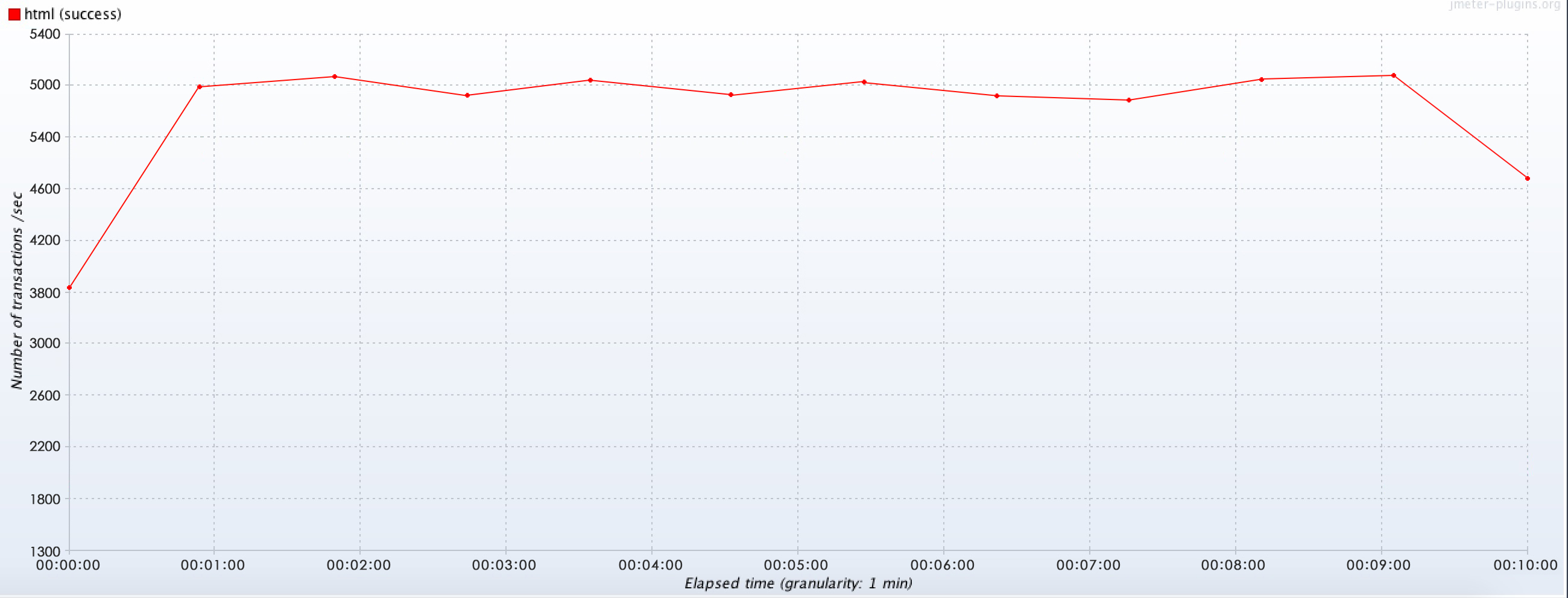
测试工具：Jmeter

测试并发：300

测试时长：10min

使用jmeter模拟300用户并发请求(时间10分钟)，每个用户在没有时间间隔的情况下提交交易请求，直到全部执行完成。记录平均事务响应时间，每秒事务数。

性能测评：并发请求返回的事务成功率、通过率为100%，根据记录得到的测试结果，经过计算与预定的性能指标进行对比，基本达到到了我们需要的结果；TPS较为平稳的固定在5000上下间。



**(2) 可用性**

**可用性要求：**可用性是一个区块链项目可靠运行的基本要求。

       QbaoChain作为区块链服务提供者，旨在为商业和组织提供区块链技术，实现高度隐私、数据安全以及性能高效的解决方案。采用POA共识机制设计，将这些解决方案与智能合约结合在一起，构成自己的"Smart Business Contract"（智能商业合约），并使用 IPFS 等去中心化存储进行相关数据存储。这就意味着从架构设计来看，这个系统的可用性考察，不仅在于底层区块链网络的可用性，还在于这些引擎的可用性，以及 IPFS 网络的可用性。

**可用性测评：**

● 目前联盟链已经上线，Github上提交代码次数达2300以上，最早提交时间为2017年12月，QbaoChain通过良好的设计原则和设计策略来实现，比如兼容性原则、模块化设计策略、安全性策略和易用性策略。

● QbaoChain区块链的交易确认速度为5秒，TPS达到最高可达5000，完全满足企业日常的需求，在增加节点硬件性能的基础上，还可以更高。

**结论：**对于定位于为企业提供区块链服务，QbaoChain极高的交易确认速度和吞吐量能满足企业的需要，同时良好的设计原则为不同企业的横向扩展提供了可能。

**(3)安全性**

**安全性要求：**作为定位于区块链服务提供者，具有业务数据上链的需要，而如何保证业务数据的安全性和业务主体的隐私性应该是重点需要考虑的方面。QbaoChain因为其授权管理，只要经过授权的节点才可以加入QbaoChain，同时因底层区块链固有的安全性保证，凸显其高安全性。

**安全性测评：**

● 联盟链的特性保证了企业的数据不对外公开，仅有授权的节点可对链上数据进行读取和修改，保证了数据的隐私性。

● 非联盟链的企业和组织可通过向QbaoChain申请授权行为，只有当绝大部分联盟成员同意之后，企业和组织才作为新的节点，共同维护联盟链的正常运作。

● QbaoChain与私有链的区别在于其部分去中心化，也正是因此，能够避免因节点故障而导致数据无法正常读取的风险，提升区块链的防护能力。

● 按照GitHub项目的部署指导手册，支持Linux、CentOS、OSX等操作系统，按照不同的部署方案实现了QbaoChain的部署，各项功能正常，性能达标。

**结论：**作为区块链服务的提供者，涉及到业务数据上链、支付等一系列业务流程，对数据安全性有着极高的要求。

**(4)架构清晰度**

**架构设计要求：**良好的架构设计不仅使得软件系统能够满足客户需求，它更为软件系统带来了安全性、稳定性、可扩展性等属性。而这些属性在应对后续业务需求变更、提供可测试性与可维护性、提高开发效率等各方面都起着非常重要的作用。

**架构测评:**

● 该项目架构采用BTC的UTXO账户模型，支持同时处理多个UTXO，因此具有良好的扩展性，可以实现并行事务并鼓励可伸缩性创新。同时将ethereum的架构进行的修改，将重复使用的功能组件化，比如：智能合约、规则引擎、BPM、非集中式资料库、非集中式档案及资料存储服务、非集中式Webhook服务，结合Tendermint技术组件进行迭代开发。

● 整体架构比较清晰，有完整的架构体系，也确保了企业商务交易高效性和高扩展性。

**结论：**整体架构基于以太坊基础之上，结合 Tendermint，规则引擎，业务流程引擎，IPFS形成了一个混合式架构。有一个比较完整的架构轮廓，各个组件有效的链接在一起，同时POA共识机制能保证授权节点的物理部署，详细的部署步骤参照部署手册。

**(5)平台币机制**

**挖矿机制：**联盟链的交易验证和区块打包是由授权节点来操作的，伴随着平台币的奖励，但QbaoChain将平台币定义为免费消耗品来使用，为提供所有节点免费获取平台币的途径，

**挖矿测评：**

● QbaoChain采用联盟节点共同维护的矿工列表进行轮流挖矿，各节点在规定的时间内无法生成区块则跳过至下一节点进行交易验证，容许一半的节点发生故障，具有较高的容错率。

**结论：**QbaoChain有其平台币挖矿机制，交易验证由授权节点完成，但平台币定义为免费使用的消耗品，QbaoChain提供获取通道，直击共有链的花费痛点，解决企业发展和开发者工作过程中成本过高的难题。

**(6)代码原创程度**

**代码原创度考察:**一定程度上体现了项目的创新性。

**代码原创程度测评：**

● QbaoChain代码基于BTC, robertkrimen, ethereum, spf13/cobra, mattn/go-sqlite3 等工程创建。

● Block和账户结构与BTC保持一致，应用平台由EVM虚拟机优化而来。

● 共识机制采用存在性证明（POA）的共识算法，联盟节点共同维护授权列表。

● 激励机制由QbaoChain实现。

**结论:**该项目代码重用了现有软件库特别是BTC和ethereum的代码实现，在此基础上添加了原创代码用以实现特有的业务逻辑，比如共识机制、激励机制等。

**4、总结**

QbaoChain于区块链服务提供者，为公司、组织等通过区块链技术落地其想法，致力于为不同商业场景提供整套解决方案。

综上所述，鉴于Github项目代码的可用性、安全性、测试覆盖测试，QbaoChain能够正常使用，挖矿功能、转账、智能合约、通证交易等功能都是正常，交易确认速度为1-5秒，TPS测试达5000+，性能优越，完全满足企业的商业场景需求。