EVOLAB

EVOLAB Benchmark

技术尽调报告

QuarkChain Testnet 夸克链测试网

（本报告不代表投资建议）

日期： 2019 年 4 月

redefine tomorrow

前言

为了让投资者透明化地了解一个区块链项目的技术情况，EVOLABTech 从共识机制、代码、安全性、拓展性和系统性能方面进行研究，推出了区块链项目的透明化技术报告 EVOLAB Benchmark。

我们的初衷是解释区块链看似复杂的技术，让人一眼了解项目的真实性能。我们根据 Github 代码、白皮书与 Benchmark 自有的技术，对公链进行分析，通过分析其技术理念是否合理，是否符和市场需求，是否能做到白皮书的设想，做出了一份反映真正技术水平的透明化代码报告。

一、 概述

Quark Chain 是一个基于分片技术的公链项目，它主要是想通过增加分片来提高系统性能。接下来，我们从共识机制、安全性、系统性能、技术管理和激励模型五个方面测试并分析 Quark Chain。

二、 分析

测试环境说明

我们的在 AWS 上部署了 30 个 Kubernetes 节点，具体测试环境如下：

	Barcelona	Paris	Tokyo	Toronto	Washington
Amsterdam	33.769ms	15.608ms	242.384ms	93.762ms	97.213ms
Auckland	339.51ms	306.857ms	262.461ms	226.613ms	227.185ms
Copenhagen	36.723ms	26.148ms	259.516ms	113.626ms	107.308ms
Dallas	136.337ms	109.758ms	134.788ms	43.671ms	45.066ms
London	25.467ms	4.001ms	235.712ms	141.819ms	84.282ms
Los Angeles	155.675ms	148.037ms	107.817ms	58.407ms	65.221ms
Moscow	78.603ms	51.796ms	221.938ms	137.391ms	126.481ms
New York	90.763ms	74.108ms	218.73ms	20.561ms	22.158ms
Paris	26.646ms	—	243.969ms	97.801ms	79.909ms
Stockholm	45.509ms	28.444ms	295.025ms	118.399ms	124.232ms
Tokyo	349.741ms	244.343ms	—	172.217ms	161.193ms

图 2-1 Kubernetes 测试环境

(一) 共识

根据白皮书以及其他公开资料， Quark Chain 采用了根链+分片结构，根链负责验证分片上的交易，分片负责打包交易。根据白皮书的描述，Quark Chain 共识机制可以理解为以下场景。我们设想有一个 100 人的议会，比特币或以太坊需要这 100 人共同讨论来决定下

一个议案，而 Quark Chain 则将其分开成为 10 个人的小议会代表团，然后可以同时提交十份议案来提高系统性能。

在一个 100 人的议会中，设定一个高级代表团（代表根链），其中有 50 人，其他 50 人仍然组成每 10 人一组的小议会代表团（代表分片）。这 5 个 10 人一组的小代表团提出的议案，积累到一定数量之后，比如 100 个提案后，交给 50 人的高级代表团，由他们验证确认。这样的方案在**提高了系统吞吐量的同时，也带了一定的安全隐患，因为总体验证的人数减少了**。比如 100 人的代表团，需要 50 个人以上才能攻击，而 Quark 的攻击只需要 25 人。

根据白皮书，Quark Chain 根链最终将采用 PoSW 共识算法，即押币挖矿，算力越大的同时，需要抵押的代币也越多。也就是说，矿工在通过哈希碰撞创造新的区块的同时，需要验证抵押代币的数量，从而计算有效算力。但根据测试网的代码来看，**现阶段仍然在采用 PoW 算法**。PoSW 的实现 demo 已经推出，代码应用目前无法评价。

而 Quark 的分片运行玻色子共识算法，其意义为允许分片（10 人一组的小代表团）使用自己的决策方式来出块。比如第一个小议会代表团采用独裁制度，也就是里面的一个人说了算。第二个小议会代表团采用轮流制，每人出块一次。这增加了区块链应用的灵活性，因为分片可以根据自己的使用场景来改变自己的共识算法。

白皮书中提到，分片之间可以进行跨链交易。但是，考虑到区块链共识算法的复杂性以及加密协议的不完全兼容性，分片之间是否都能安全的实现跨链交易，这里可能还是会存在一定的限制。由于目前玻色子共识算法还没有实现，所以这部分也是未来可能的问题。

(二) 安全

通过 Benchmark 公链测试工具，我们对 Quark Chain 进行一系列安全测试，并从中选取了我们认为对该公链来说，有参考意义的几个攻击指标。

我们的测试方法如下:

1. 建立 Quark Chain 测试网；
2. 发送 RPC，让测试网部分节点对其他节点发起攻击；

得到测试结果如下：

表 2-1 Benchmark 安全测试结果

方案	结果	备注
女巫攻击	通过	模仿出多种身份进行的攻击
BGP 劫持攻击	不通过	通过破坏使用边界网关协议（BGP）维护的路由表非法接管 IP 地址组
网络带宽服务攻击	不通过	通过耗尽网络带宽资源使得网络无法正常工作

测试结果：Quark Chain 可以抵御女巫攻击,**满足一个公链项目的基本安全需求**，但无法抵御 BGP 劫持攻击和网络带宽服务攻击。

(三) 性能

通过 Benchmark 公链测试工具，对 Quark Chain 进行性能测试，测试方法如下:

1. 建立只包括单分片的 Quark Chain 测试网;
2. 发送 RPC，让测试网部分节点发起交易(每秒 N 笔交易，线性增长);
3. 节点检测交易同步的时间，直到检测到超过一定时间(一般是出块时间)

测试结果：Quark Chain 单分片的 TPS 为 50。因为 Quark Chain 采用分片技术，**理论上只需要可以通过增加分片，提高系统吞吐量。**

(四) 技术管理

1. 代码更新

Quark Chain 的 Github 仓库的一共有 4 个 public repositories，每个 repositories 的具体数据如下:

表 2-2 QuarkChain 的 Github 数据

repositories	description	commits	Watches	stars	forks
pyquarkchain	Python implementation of QuarkChain	1312	36	157	92
quarkchain-web3.js	QuarkChain client library built around web3.js	42	8	18	10
tqkc-bounty-lottery	-	12	4	2	2
crowdsale-whitelist	-	9	4	22	56

根据 Quark Chain 的 pyquarkchain 的 commits 数据，得到 pyquarkchain 的代码更新，如下：

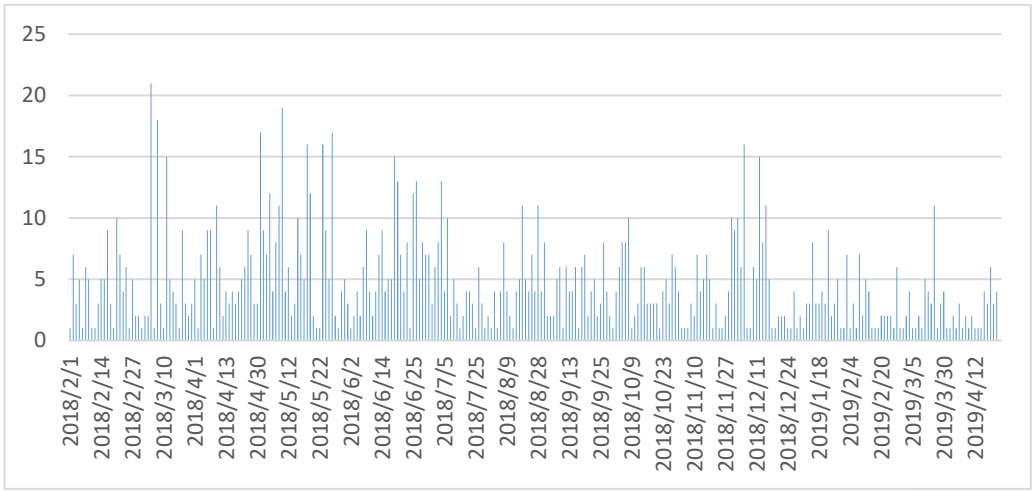

图 2-2 pyquarkchain 的代码更新情况

说明：pyquarkchain 代码也在一直持续更新，相对于 Coinmarkcap 排名附近的其他项目，也算是更新比较频繁。

2. 代码重复度

通过 Benchmark 公链测试工具，我们对 Quark Chain 进行代码相似度检查，我们的测试方法如下:

(1) 建立代码索引库

(2) 把目标代码放进 Elasticsearch

(3) 把目标代码和其他代码作比较

测试结果：我们发现 pyquarkchain 部分代码**和 pyetherum（以太坊）高度重合**，可以判断 pyquarkchain 借鉴 pyetherum 的思路进行开发。

(五) 激励模型

QuarkChain 采用挖矿激励，有两种挖矿方式，一种是根链挖矿，另一种是分片挖矿。根链挖矿主要负责验证交易，除了得到根链挖矿的奖励外，分片出块会向根链交一定的“税”作为对根链矿工的奖励。分片挖矿则主要是负责打包交易。

三、 总结

QuarkChain 共识和分片方案是借鉴 Ethereum 的思路，开发也借鉴了 pyethereum 的代码。类似的分片方案在以太坊上也有讨论，比如 Layer 2，从技术设想上看，是**通过牺牲安全性以提高系统性能，没有算法级别的挑战**，但如果能在工程上实现的好，对社区和市场也是有价值的。

https://evolab.io

@EVOLABTech

https://twitter.com/EVOLABTech

https://www.weibo.com/u/6560757147

https://medium.com/@EVOLAB

https://www.facebook.com/EVOLABTech/

http://t.me/EVOLAB

https://github.com/EVOLABTeam

contact@evolab.io

技术驱动，加速区块链初创团队成长