

泰山沙盒云

产品技术实施案例介绍



天民（青岛）国际沙盒研究院

2018年10月

目录

一、沙盒云测评与监管技术概述:	2
1.1 测评技术概述	2
1.2 监控技术概述	3
二、测评技术实施案例	3
2.1 测试环境	3
2.2 测试平台实施自动化测试任务	4
2.3 测试结果与分析	9
三、监控技术实施案例	12

沙盒云产品技术实施案例介绍

一、沙盒云测评与监管技术概述：

沙盒云测评与监管技术根据区块链特点，通过合理的设计与规划理论上可适用于任何区块链产品的测试与监管。沙盒云底层采用通用云计算技术结合区块链节点集群私网环境自动编排技术加以实现，测试与监管技术层对各区块链协议与功能性进行共性特征的抽象与提取，采用模块与插件式设计加以实现，为区块链沙盒服务提供了共性技术支撑的基础性平台，可根据各区块链测试与监管的特殊性需求，花费很少的代价进行基于沙盒云产品平台的插件开发，理论上可以适用任何区块链的测试与监管。

1.1 测评技术概述

在传统软件自动化测试技术的基础上，根据区块链的节点分布式部署、交易共识机制、对等网络通信、对外提供接口方式（业务接口与编程接口）等特点实现了针对区块链的接口功能和性能的自动化测试技术：

- 普适性架构

对区块链进行共性特征的抽象与提取，形成微服务与模块化架构设计方案，测试平台支持插件式的测试组件扩展，从而达到快速适应各类不同区块链测试的能力：

- 分布式调度与结果实时统计分析技术

利用分布式测试通信与任务调度技术，流式并行计算框架等，测试平台可动态扩展测试实施规模，并在测试执行中，实现大量测试数据的实时结果统计与分析：

- 性能指标监控技术

实现针对区块链特有性能指标（出块效率、交易入块效率、滞留交易堆积率等）的监控方案，并以测试组件方式与测试平台集成，服务于区块链性能测试；

- 测试全生命周期管理

形成以接口契约模型为测试最小管理单元的测试管理技术方案，测试平台可对测试全生命周期进行有效管理，支持测试对象管理、测试用例设计、测试数据自动生成、测试任务配置与执行、测试结果分析，测试报告生成等功能。

1.2 监控技术概述

根据区块链分布式链路与共识机制的对等网络数据交互场景，实现了在区块链私网环境下跟踪和监控整个节点网络集群的共识与交易技术：

- 区块链分布式共识与交易过程链路跟踪技术

形成分布式链路跟踪技术，实现跟踪和采集区块链集群网络节点间的共识与交易数据，从而达到直观的监控到整个共识算法的流程、交互数据内容和步骤以及交易的广播网络路径的目的；

- 跟踪技术规范与 PRC-API

形成统一的跟踪技术规范与 PRC-API，实现对多种编程语言（Java、C#. NET、NodeJS、Golang 等）区块链的监控支持；

- 跟踪数据收集与分析技术

形成对分布式跟踪数据的高性能收集与分析技术，完成对数据的实时分析与聚合，并可通过分析自动构建区块链共识与交易过程的网络交互拓扑图和检索共识与交易过程细节数据。

二、测评技术实施案例

我们分别选区了区块链项目 A 和区块链项目 B，通过沙盒云所提供的测评技术完成测试任务。

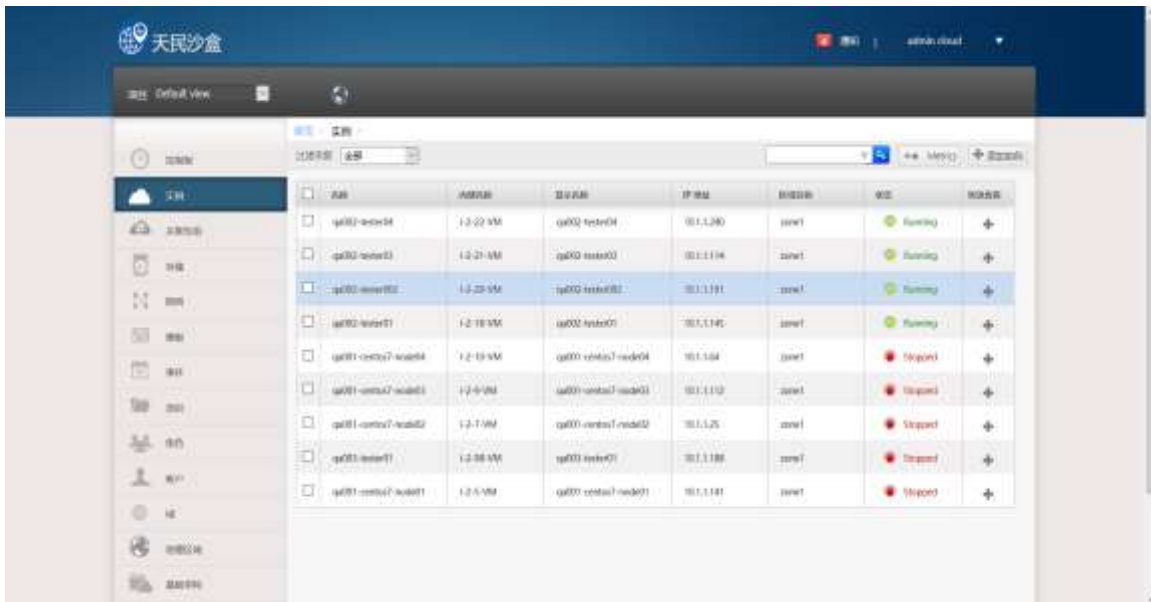
2.1 测试环境

首先，通过混合云基础设施，利用构建区块链模板镜像的方式，快速搭建起区块链私网节点集群测试环境。

我们在实际操作中启动 4 个区块链项目对应的虚拟机实例，加载对应的模板

镜像，并使用自动编排技术进行对 4 个节点的协议、资产与网络的配置工作，自动化地完成对应目标测试环境的搭建任务。

下图为利用天民沙盒启动测试环境的过程：

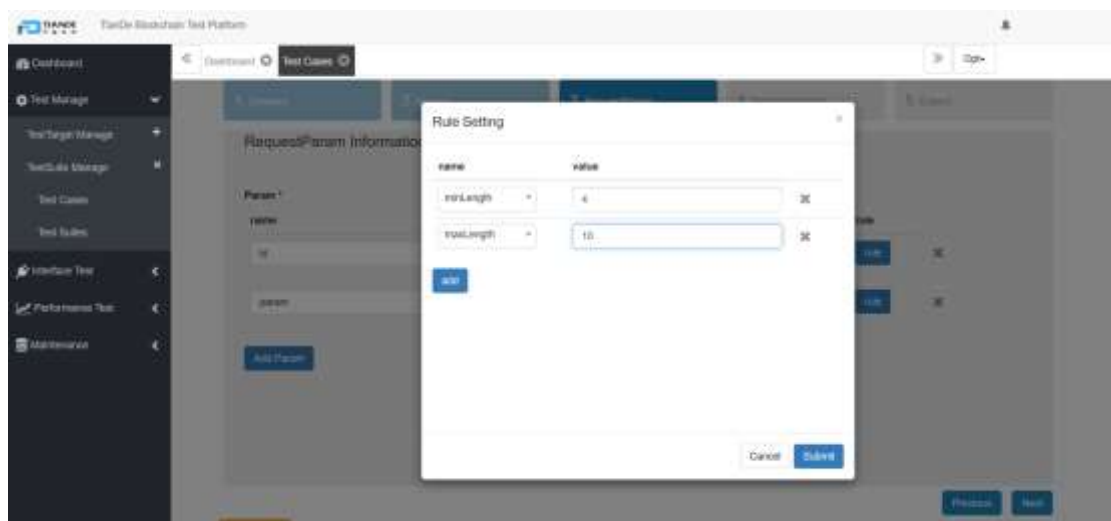


2.2 测试平台实施自动化测试任务

通过天德区块链测试平台完成对目标区块链 A 和区块链 B 的接口功能与性能测试。

接口功能测试的具体实施如下过程：

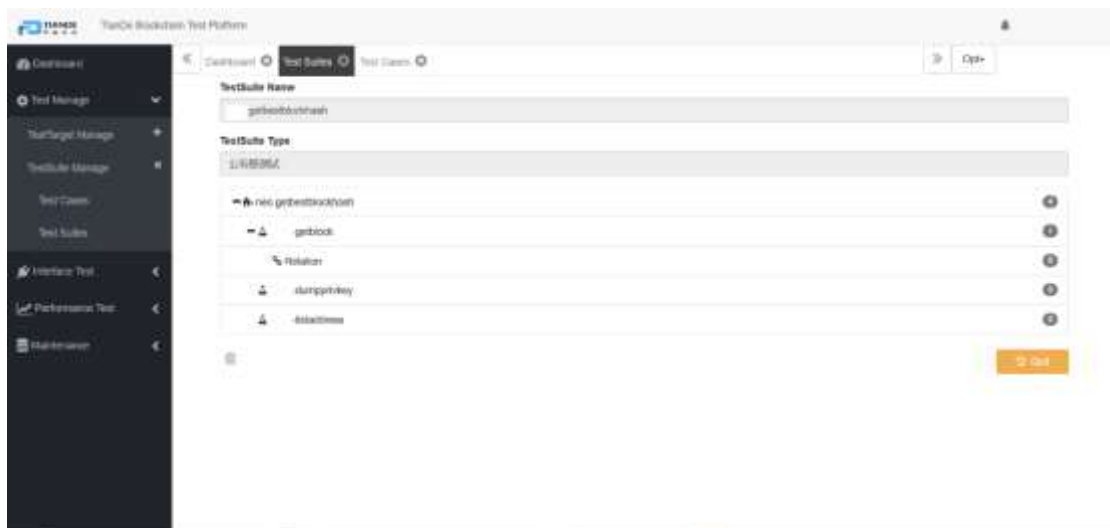
- (1) 对应目标区块链所提供的所有接口服务，创建契约模型测试用例，测试用例中可通过对参数的规则设置自动生成测试数据，创建测试用例如下图所示：



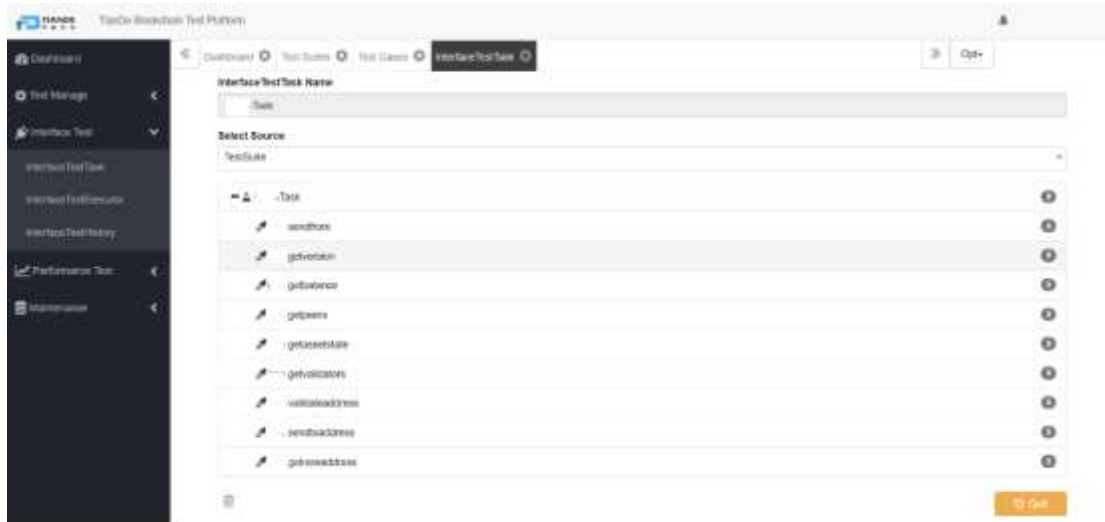
(2) 通过对测试用例的管理，查看已经建立的测试用例内容，如下图所示：



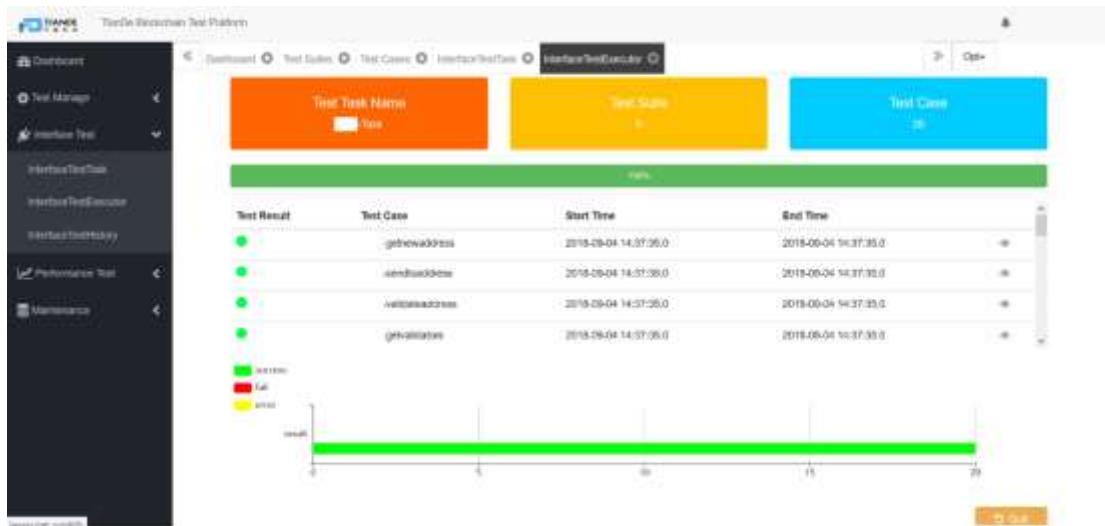
(3) 对应目标区块链的被测试功能项，将通过配置测试集进行完成，测试集将测试用例按照步骤和关联关系进行有机结合，从而完成一个区块链的具体功能业务，如下图所示：



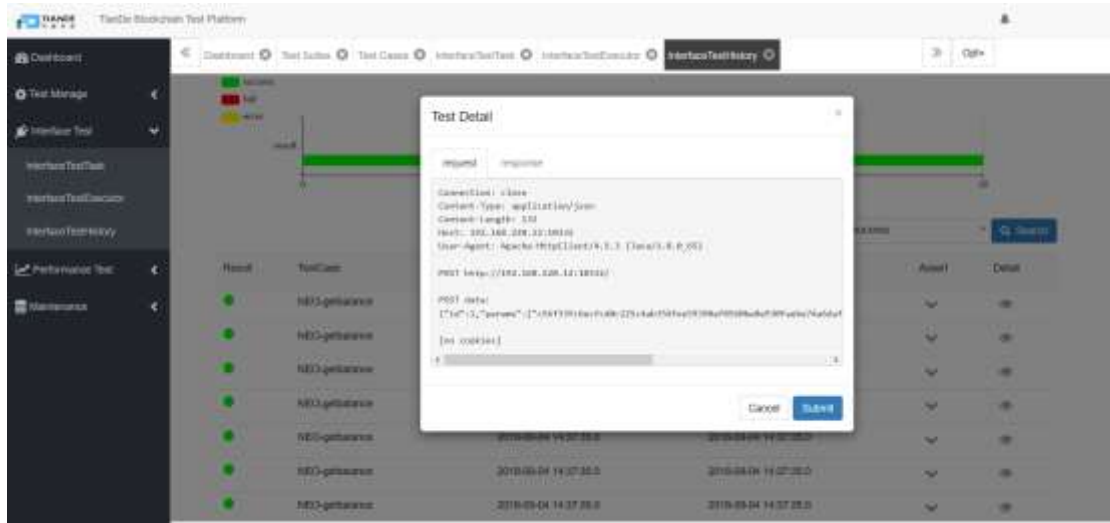
(4) 通过配置接口测试任务，可将目标区块链的所有测试集进行汇总，可一次性完成全部接口功能的自动化测试，如下图所示：



(5) 启动测试任务，完成自动化测试，测试中可实时返回测试结果，如下图所示：



(6) 测试后可以查看测试任务执行的历史记录，如下图所示：



性能测试的具体实施如下过程：

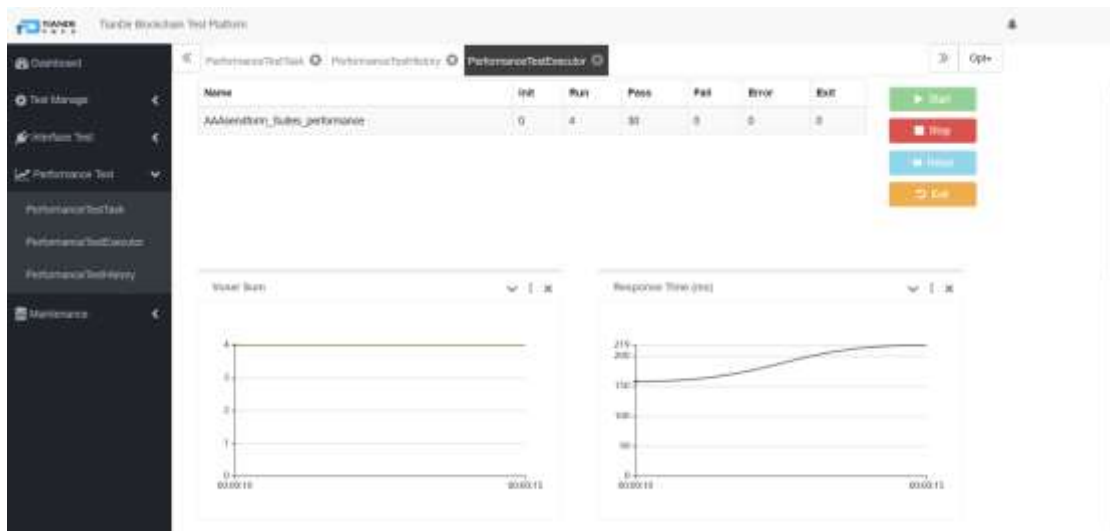
(1) 根据性能测试需求，创建对应的性能测试任务，如下图所示：



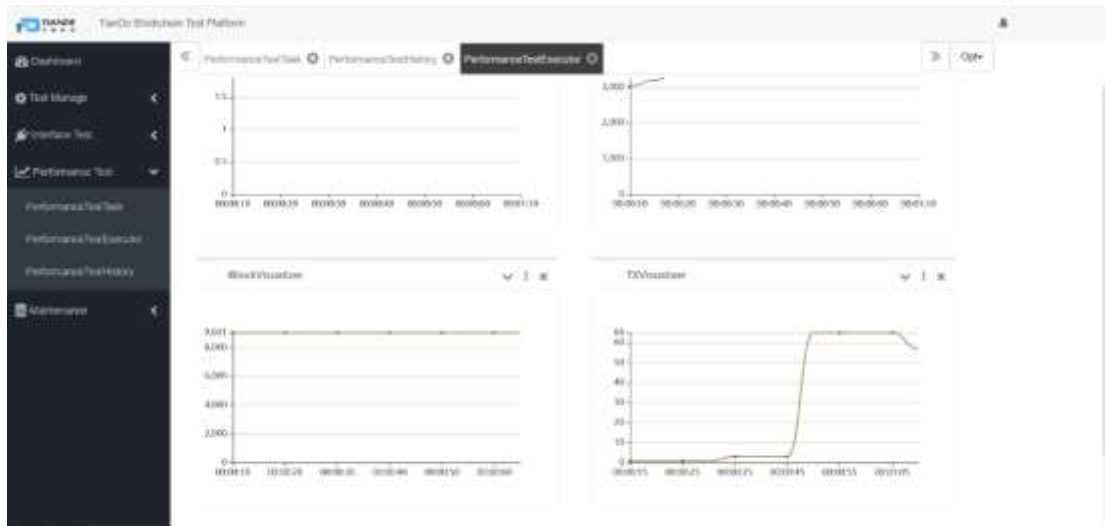
(2) 通过对测试任务的管理，查看已经建立的测试任务内容，并设置分布式性能测试主机参数，如下图所示：



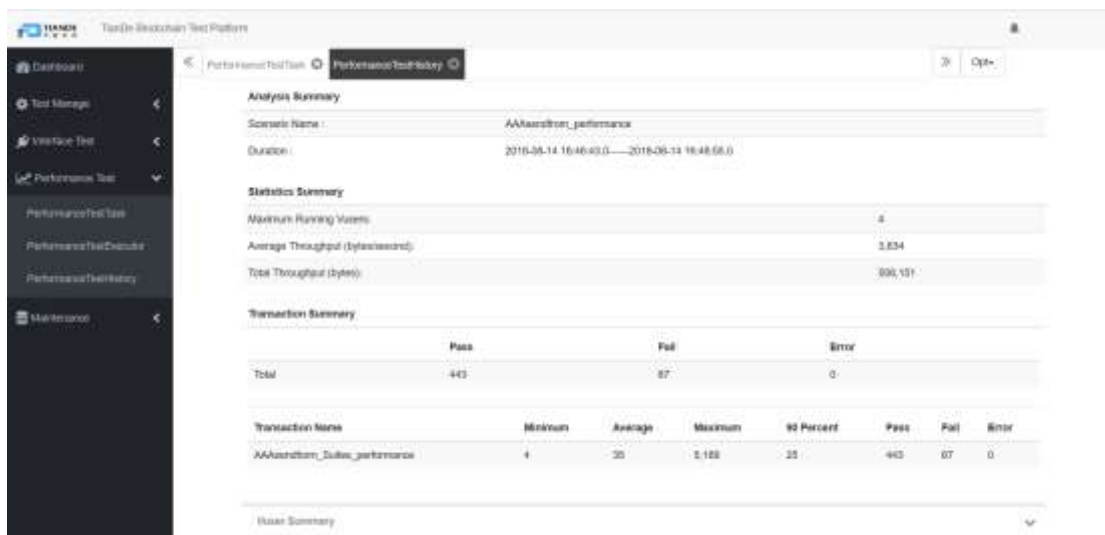
(3) 启动测试任务，完成自动化测试，测试中可实时返回图表内容的测试结果，如下图所示：



(4) 测试执行中，可对被测试区块链的出块效率和交易 TPS 进行实时监控：



(5) 测试后可以查看测试任务执行的历史记录，如下图所示：



2.3 测试结果与分析

(1) 功能测试结果

测试项	测试子项	测试内容	区块链 A	区块链 B
基本功能	加密体系	密码算法	通过	通过
		地址	通过	通过
		消息加密与解密	通过	通过

		签名与验签	通过	通过
	共识机制	块设计	通过	通过
		共识算法	通过	通过
			通过	通过
			通过	通过
		加入共识	通过	通过
	退出共识	通过	通过	
P2P 对等网络	对等通信	通过	通过	
	网络发现	通过	通过	
链功能	账户	外部拥有账户	通过	通过
		合约账户	通过	通过
		账户地址	通过	通过
			通过	通过
	隐私保护	通过	通过	
	交易	转账	通过	通过
			通过	通过
通过			通过	
广播	通过	通过		
入块	通过	通过		
节点客户端	完整节点	完整区块链	通过	通过
			通过	通过
		网络路由表	通过	通过
	块服务	根据指定的散列值，返回对应的区块信息	通过	通过
		高度最大的区块的散列	通过	通过
		根据指定的索引，返回对应的区块信息	通过	通过
		区块的数量	通过	通过
		指定的索引，返回对应区块的散列值	通过	通过
		指定的索引，返回截止到该区块前的系统手续费	通过	通过
	交易服务	未确认的交易列表	通过	通过
	钱包服务	密码加密钱包	通过	通过
		钱包锁	通过	通过
		备份与恢复	通过	通过
浏览器	Blockchain 浏览	块信息	通过	通过
		交易信息	通过	通过
		账户信息	通过	通过
		合约地址	通过	不通过

	智能合约浏览	合约交易	通过	不通过
		合约源码	不通过	不通过
	节点浏览	节点信息	通过	通过
	市场浏览	市场信息	通过	通过
	竞选与投票信息	投票统计	通过	通过
		投票产生	通过	通过
		竞选信息	通过	N/A
Token 浏览	Token 信息	通过	不通过	
智能合约	生命周期	可部署	通过	通过
		可验证	不通过	通过
		可触发	通过	通过
		可终止		通过
		可见	不通过	不通过
	多重签名	签名	通过	通过
		验签与执行	通过	通过
	非图灵完备	智能合约支持参数配置	通过	N/A
	图灵完备	智能合约支持一种或多种合约语言	N/A	通过
	虚拟机	编译字节码	不通过	通过
		执行字节码	不通过	通过
	开发支持	开发工具	不通过	不通过
		合约模板	通过	不通过
测试支持	测试网络	通过	通过	

(2) 性能测试结果

测试项	测试内容	区块链 A	区块链 B
出块效率	出块效率	10s	16s
最大 TPS	TPS	23TPS	15TPS

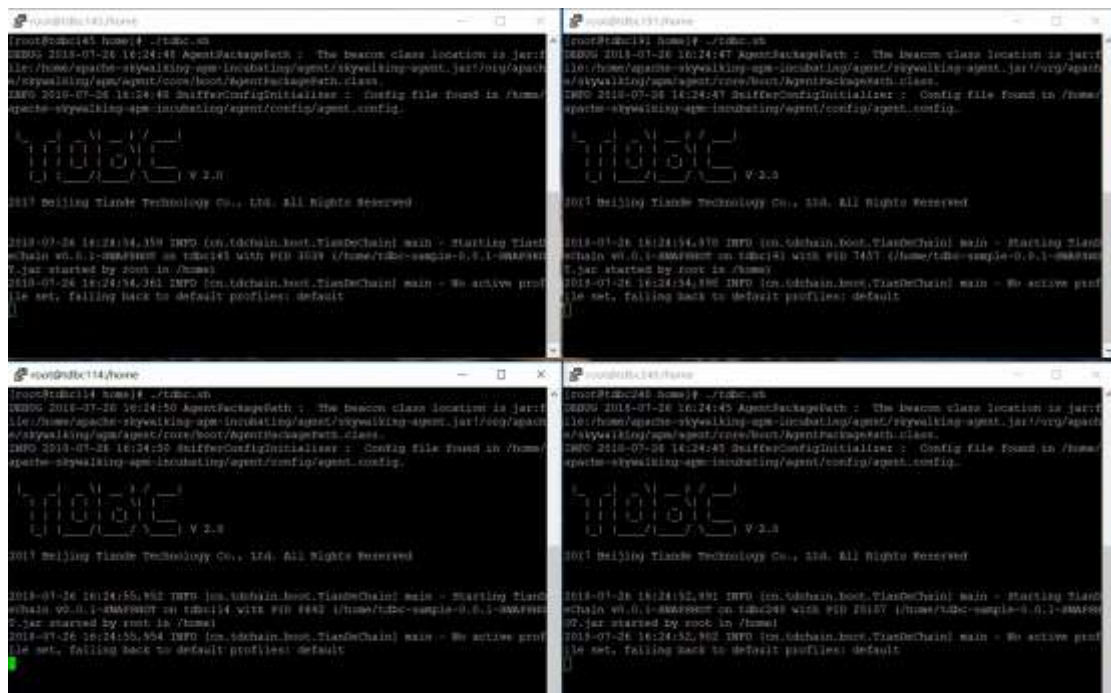
根据上述测试实际结果我们进行分析,功能方面通过分级指标模型得到区块链 A 在智能合约方面的技术能力较弱,在整体 5 个级别中处于 2、3 级之间;区块链 B 在区块链浏览器方面的技术能力较弱,在整体 5 个级别中基本达到 3 级。性能方面两个区块链均未达到其白皮书中的 TPS 理论最大值,出块效率基本与白皮书中的理论值一致。

三、监控技术实施案例

我们在对区块链共识算法和机制的测试过程中，通过监控系统监控整个区块链节点网络集群的共识过程，进行分布式事务链路跟踪，从而可直观的了解整个共识算法的流程、交互数据内容和步骤等，可辨别区块链共识机制与其白皮书的相符程度。

(1) 启动区块链共识网络

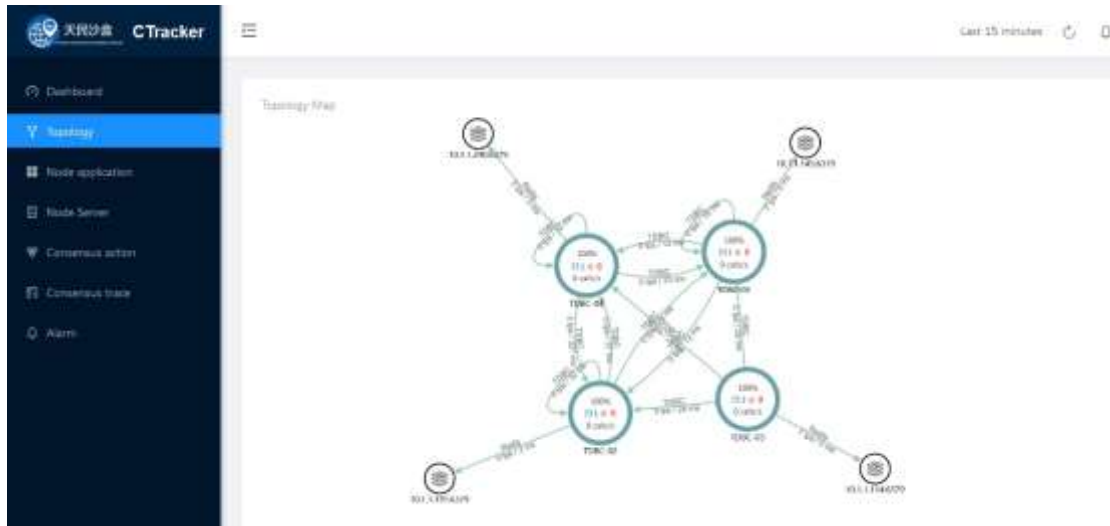
我们同时启动 4 个区块链节点，形成区块链共识网络，在共识网络建立后，利用测试平台进行交易转账的性能测试，制造大量的交易事务，如下图所示：



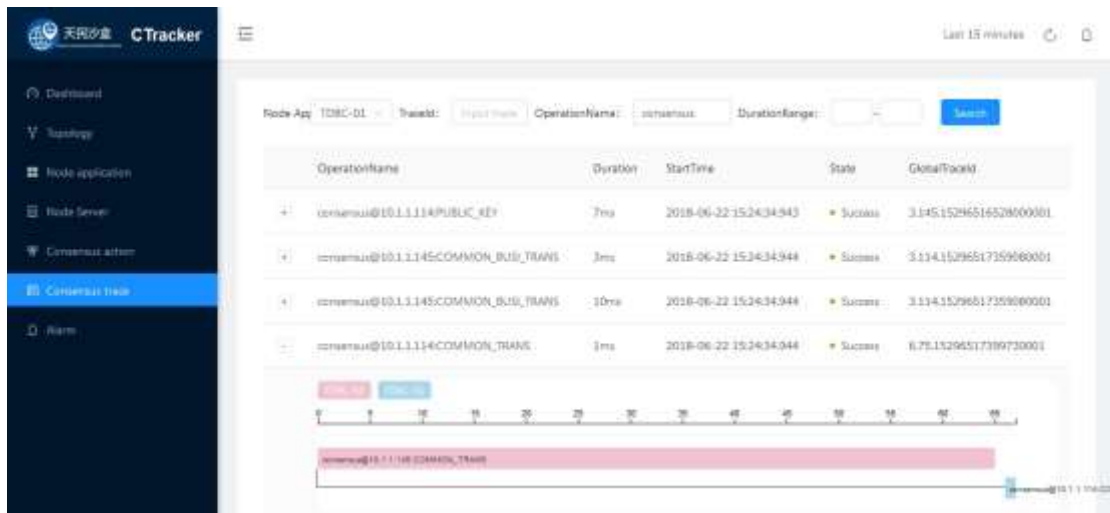
(2) 共识与交易跟踪监控

启动共识与交易跟踪监控系统，以下为区块链共识与交易跟踪监控系统的主要功能演示：

- 可自动探索整个区块链节点集群的共识交互拓扑图



- 可对共识过程的阶段、过程和数据进行追踪



- 可对共识节点的状态进行监测

