第 3 卷◆第 5 期◆版本 1.0◆2020 年
文章类型：论文|刊号（ISSN）：2630-4759 /（中图刊号）：270GL018

区块链的可运维性的相关研究

童长卫
中共龙岩市委党校
DOI:10.12238/ej.v3i5.563

[摘　要] 传统IT系统生命同期分为规划设计、开发建设、运行维护三个阶段。运行维护是产生价值的阶段,是时间周期最长的阶段。传统IT运维一是要是预防系统可能发生的错误,二是不断完善系统功能,三是在系统发生故障时能快速恢复,保证系统的正常运行。传统IT运维有专门的组织(个人)负责。而区块链的特点是去中心化,它的运行模式是全新的。本文围绕区块链要不要运维、由谁运维、怎么运维展开讨论,提出了自己的看法。
[关键词] 区块链；可运维性；研究
中图分类号：F830.9　文献标识码：A

1 传统IT与区块链的可维护性分析

1.1传统软件与区块链质量特性分析

传统软件的质量特性。GB/T16260.1-2006对软件产品的质量特性有明确定义,共6大特性21个子特性,主要包括软件的功能性、可靠性、可用性、效率、可维护性及可移植性。

1.2区块链的质量特性

区块链做为一种分布式的记帐系统,通过密码学理论保证帐本的不可篡改和不可伪造。它与传统IT系统最大的区别是去中心化。因此,衡量区块链系统的质量特性除了上述6大特征与21子特性外,至少应增加一个可信性。可信性主要包括两个子特性：

(1)秘密性。由于区块链的数字基础是密码学。因此,区块链所用加密系统公钥与私钥的不可破解性是区块链可信性的一个重要指标。另一方面,哈希运算在区块链中有着重要地位,因此,哈希算法的空间复杂度和时间复杂度也是区块链的一个重要指标。

(2)公平性。区块链的帐本记录在分散的各个节点中,如何使分散记录的帐本保持一致,共识机制是关键。因此,一个好的区块链它的共识机制一定是公平的。公平具有两重意义,一是大家面对同样的游戏规则,二是不会为大公司所垄断。比特币原本是去中心化的,但由于采用了工作量证明机制,权力由算力决定,这使得比特币的发展逐步形成了以比特大陆、蚁池为代表的权力中心,这违背了中本聪创立比特币时的思想,对于比特币的长期发展不利。

1.3区块链的可运维性

传统IT的可运维性主要由系统的可靠性和可维护性等质量特性所决定的。而区块链的的运维有自身特殊性,它与传统IT的区别主要有：

(1)区块链的可恢复性。可恢复性是指系统损害后恢复系统(特别是恢复数据)使系统重新正常运行的能力。区块链采用去中心化的分布式数据存储,每个节点独立运行系统。虽然它的稳定性较有保证,但也不排除系统遭到损坏的可能。比如,区块链网络遭到大规模的网络病毒攻击,大部分节点瘫痪或大部分节点的数据被篡改。由于区块链没有传统意义的数据中心,因此也没有传统意义的灾备中心,此时,区块链应如何恢复?这是衡量区块链可靠性的重要考量。一个好的区块链应有好的应急方案,这可以通过考察区块链的白皮书及实际操作进行测试与评价。

(2)区块链的监控。一个可运维的系统一定是具备监控功能的,否则无法了解系统的运行状态,更谈不上运维。区块链是去中心化的,一般不存在运维中心。不可能设置特别的专用的只有特殊用户才具有的监控权限,更不可能赋予运维人员选择性关停、限流等应急操作的权利。因此,区块链的监控平台一定是开放的。在没有监控管理中心的情况下,如何实现区块链的可监控、可管理这是区块链可运维必须面对的难题。

2 区块链的可运维性存在的问题

区块链是一个集密码学、分布式储存智能合约、共识算法等多种新型技术为一体的数据传输与存储方式,能为用户提供信任服务。近几年,随着区块链技术的快速发展,区块链的可运维性也开始得到了人们的关注。

2.1区块链运维的必要性与迫切性

在应用区块链技术时,不能只看到区块链技术不可篡改、不可伪造的高可靠性,从而忽视了区块链的可运维性。以目前情况来看,虽然区块链技术得到了快速发展,但是能够为区块链的可运维性提供的技术支撑少之又少,而且通过以往在区块链的可运维性遇到的问题中,可以看出区块链的可运维性不仅需要以传统的软件管理的理念和做法为基础,还要根据区块链的特点研究新的运维管理理念和办法,特别要注意改正之前区块链

领域的错误理念和做法。另一方面，由于区块链是开源的，同时可能涉及价值巨大的数字货币，是最容易遭受黑客攻击的系统。因此，系统的运维问题更显重要。

2.2区块链的运维组织

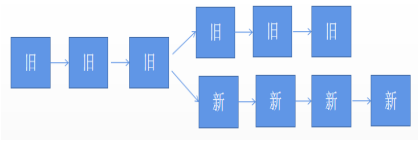
联盟链与私有链的运维组织容易解决，但公有链的运维该由谁负责？

在一条公有链发布之初，它的规模较小、影响也较小。它的初始运行阶段实际也是实测阶段，可能各种问题，此时的运维只能由发布者承担。随着这条公链的运行，参与的节点可能越来越多，影响也越来越大。为体现区块链的去中心化，区块链的发布者应逐步退居幕后。中本聪在比特币发布后采取主动“消失”的手段是很有意义的。为了保证区块链的正常行与不断发展，应该成立相应联盟或协会组织。联盟或协会的成立应有广泛性和代表性，不能由少数大公司垄断。区块链的运维可由联盟或协会负责组织，所有成员共同完成。

2.3协商机制

由于区块链的去中心化，没有形式上的运维中心。但有些技术团队由于技术的优势渐渐成为事实上的“技术中心”，就像比特币的Bitcoin Core团队。他们开发和更新bitcoin core，定期发布新版本，最终比特币网络里的节点再去更新逐渐完成整个比特币网络的升级。但这些“技术中心”并没有权力去强迫其他节点用户采用他们的新版软件，因此，为保证全网大部分节点接受，必须采用协商机制。在推出新版本时必须遵守以下两个原则：

(1)保持链的一致性。引入新的协议后，如果有部分节点不愿更新，他们不承认(验证不通过)新版本节点所挖的块，这样链就会出现分叉－－－硬分叉。如下图：



这样的更新实际上产生了新链，不是对原有链的维护。比特币就产生过硬分叉，在2017年8月，由ViaBTC领导的矿工团体创建一个比特币分叉——Bitcoin Cash(简称BCC或BCH)。

所以引入的新协议应保证，即使有部分节点不愿更新，但他们能承认(验证通过)新版本节点所挖的块。这样即使链上存在新旧多个版本也不会产生新链。

(2)保证原有价值。区块链是有价值的。新的版本要保证原链的价值，也就是要保证原有节点的权益。否则，新的版本肯定得不到原节点的承认，仍然会造成区块链的分叉。

3 区块链的可运维性相关建议

3.1区块链的合规性

“我的资产我做主”这绝不是一个与现行法律体系完全相符的理念。如果在技术上可以实现“我的资产我做主”，而“做主”在技术上的体现应该就是自己“掌握私钥”，但是这种技术在一些特殊的场景下就不能很好的执行法律的要求，在解决任何问题时都要首先考虑区块链的技术设定。这在发生突发情况需要处置时，这种掌握私钥的技术在法律上存在明显的缺陷。因此，在区块链技术应用过程中把执法措施落实到位是区块链单位符合相关法律规定以及要求的基础。在只是借鉴区块链技术为主的阶段可以忽视法律合规性，但是当区块链技术进入自主创新、自我掌控阶段时，在应用过程中就要重视符合相关法律的规定。

3.2将运维目标纳入开发过程中

开发方要明确用户对可运维性的要求。一是在进行区块链开发部署时开发方要注重形成自己的模板，把具有共性的可运维性功能作为模板的标配，嵌入区块链的开发部署中。二是开发公司要建立完善的业务约束标准，这个标准要基于业内可运维性的理念以及以往的经验积累，把关键业务中具有共性的地方固定下来从而应用到模板中。三是联合具有相同运维理念的开发企业，建立共享性质的可运维性模板，以此来提升区块链的可运维性功能，减少研究过程中的误区。

3.3严格准入制度

有缺陷的区块链应用的上线对用户来说是一件非常危险的事情，而且不只是对自身的用户群和业务生态产生影响，由于跨链操作的存在还会对其他的链产生影响。当链的应用范围不断扩大时，对于承载重要业务、运作重要资产的区块链一定要采用严格的应用准入制度，不但要自带某种形式的验证过程，还要具备应急处置功能，以此保证区块链应用的可靠性。

3.4加强运维研究

区块链的可运维性在法律与技术层面都存在许多空白。必须加强这方面的研究投入，建立我们国家自己的区块链运维标准与运维体系。同时还要加强区块链可运维重要性的宣传，培养这方面的人才，这样才有助于区块链的健康发展。

4 结束语

可运维性是目前区块链发展所面临的重大问题，如何在法律法规及技术层面完善区块链的可运维性是关系到区块链能否大规模应用的关键技术之一，必须引起高度重视。

[参考文献]

[1]白硕.浅论区块链的可运维性[J].大数据,2018,4(1):85-89.

[2]刘蕾.区块链技术在金融领域的应用与合规监管[J].管理现代化,2020,40(3):10-12.

[3]邵奇峰,金澈清,张召,等.区块链技术:架构及进展[J].计算机学报,2018,41(005):969-988.

[4]赵妍.浅析区块链的发展与未来[J].消费导刊,2019,(043):222-224.