浅论区块链的可运维性

Brief comments on the operability of blockchain

白硕(1956-),男,中国分布式总账基础协议联盟技术委员会主任,中国科学院计算技术研究所博士生导师,资深金融科技专家,上海证券交易所前总工程师。主要研究方向为区块链、金融科技、大规模内容处理和网络安全等。

中图分类号:TP315 文献标识码:A doi: 10.11959/j.issn.2096-0271.2018009

1 引言

什么是IT系统的“可运维性”？通俗地讲，IT系统的可运维性就是一个IT系统自身提供的确保该系统的正常运行状态、排除该系统的异常运行状态、应对突发的运行需求的能力。这种能力最终需要与从事运维工作的人结合，才能真正发挥其预期效果，但是如果系统提供的“可运维性”能力很差，就会导致从事运维工作的人无处发力或者只能用非常低级原始的办法实现运维目标。从这个意义上讲，IT系统的可运维性是其得以安全、平稳、高效运行的前提。

2 可运维性对金融机构的重要性

笔者在传统金融行业从事过多年IT运维管理工作，深知可运维性对金融机构的重要性。其重要性具体体现在以下几个方面。

（1）确保系统正常运行状态的主要途径是架构手段

通过高可用架构实现尽量短的故障恢复时间目标（recovery time objective，RTO）和可容忍故障恢复点目标（recovery point objective，RPO）。很多关键业务系统的RTO为秒级，RPO为0，这意味着不允许任何数据丢失和业务状态错乱，业务的短暂中断不会使普通用户感觉到明显停顿。为此，在高可用架构中要有大量的冗余设计和接管（failover）措施，从机房、电力、网络、主机、存储、数据库、中间件、域名解析到应用，都需要在架构设计上一体化考虑，都不允许出现单一故障点。

（2）排除系统的异常运行状态是监控手段和应急操作特权入口

提供详尽、可理解、可视化的直观监控信息，可帮助运维人员实时了解系统和网络的真实健康状况，以便及早发现并应对异常；提供应急操作特权入口，可为改错、选择性关停、限流等应急手工操作提供一个安全方便的操作环境。

（3）应对突发运行需求的主要途径在架构层面是参数化设计，在操作层面是保留最终干预权

灵活的参数化设计可在短时间内通过参数调整应对突发的业务改变。比如2015年，证券市场的“熔断”机制推出后数天即被叫停，借助于参数化设计的这种灵活性，技术系统仅仅需要把熔断触发条件设置成逻辑上不可能的参数值就可以很快满足这一突发的运行需求。最终干预权则是对关键业务系统的核心模块提供人工干预的应急接口，是满足突发运行需求的操作。需要注意的是突发运行需求的起因并不是系统发生了异常，而是系统运行的宏观外部条件（如政策）发生了异常，迫使系统必须以非常规的手段进行应对。

3 区块链的可运维性问题

区块链是一种基于密码学和分布式共识机制、为一个特定用户群提供信任服务的基础设施。近年来，区块链技术得到了迅猛发展，不仅在民间有基于“虚拟货币+社区+区块链平台”的“币圈”打法，在传统金融机构和其他行业也出现了仅利用区块链平台服务于业务目标的“链圈”打法。随之，区块链语境下如何体现可运维性也开始浮出水面。

不要以为区块链技术从其架构本性上来讲就是高可用的，因此就可以忽视可运

维性的问题。实际上，区块链技术发展的现状为区块链可运维性提供的技术资源非常少。从区块链领域遇到的大大小小涉及可运维性的问题中，笔者深深地体会到，区块链的可运维性既需要大力度借鉴传统金融机构管理可运维性的一系列理念和做法，也需要基于区块链语境本身的特殊性发展一系列原创性的运维管理做法，尤其是要纠正区块链领域的一些错误的认识和做法。

2016年“The DAO事件”余波未平，2017年以太坊又爆出了Parity多重签名合约误锁漏洞。区块链的可运维性又一次引起热议。2016年比特币社区还在嘲笑以太坊社区一言不合就分叉，2017年分叉的事情就轮到了比特币社区。每次看到社区出现这样的情况，总会有传统金融机构的人说：“看看，幸亏‘链圈’没有这么玩，否则指不定死多少回了！”

其实，可运维性不仅是“链圈”追求的区块链特性，也同样是“币圈”追求的区块链特性。在解决了不可撤销、不可仿冒、不可篡改、不可抵赖、不可双花、不可透支这些价值传输最基本的问题之后，人们的目光停留在了隐私保护和可运维性上。说起隐私保护特性，“币圈”有ZCash这样的虚拟货币推出。可运维性方面，也许是去中心化的观念先行，排除了大量在“币圈”看来很平常的运维手段的使用，从应急处置和审计追责的角度，还没有看到“币圈”有份量的可运维性技术的推出。但是，从预防为主的角度来看，至少智能合约的形式化验证问题和在线升级的问题已经在“币圈”引起了足够的重视，这一迹象是正面的。

在这里必须提到“链圈”的两个值得一提的努力。

一是埃森哲公司提出的“可编辑的区块链”概念。在埃森哲的材料中，他们开宗明义，将可编辑区块链的推出与传统金融机构的可运维性需求挂钩，从不当得利、错账冲正到乌龙指，各种必须修改的错都不能将错就错，需要得到授权的操作人员把错账改过来。如果区块链承担了记账的任务，那么改错账就应该是区块链必备的功能。以比特币、以太坊为典型代表的“币圈”平台做不了这件事情，除非分叉。埃森哲提出的解决手段则是使用基于“变色龙散列”的“可编辑的区块链”。从数学原理上看，可编辑的区块链确实可以不分叉就能改错，但是代价是开了一个既能篡改历史又不可审计的后门。这样一个后门的存在，不仅在坚定秉持去中心化理念的“币圈”不可接受，就算是在一定程度上容忍中心化要素存在的“链圈”，接受的人也不是很多。

二是分布式账本联盟R3在2016年底推出的Corda平台。在Corda平台上，智能合约代码和对应该合约的正式有效的法律文本是互相勾稽的。合约法律文本的存证形态是合约代码不可缺少的附件，并以数字签名存证。通过对附件的验证，给予合约代码所代表的“本意”一个抓手。一旦合约在运行中出现问题，至少可以通过查验来确定是法律合约原本就有的，还是由合约的代码实现没有忠实地体现法律合约的“本意”造成的。在某种程度上，这也算是对前一段时间合约代码单兵突进、法律法规没有同步跟进，结果形成畸形生态的一个弥补。此外，Corda平台上并不存在一个“我的资产我做主”的基础账本，任何单据（状态）都可以在合适的条件下经公证被废止。这也为改错账留下了可以运作的空间。可以说R3这些业务大咖们对分布式账本可运维性的重要意义还是心中有数的。

4 提出的建议

可运维性的诉求是一个很重要的诉

求，它在“币圈”的缺位不是因为“币圈”不需要它，而是因为“币圈”有难言之隐，在目前技术条件下无法把这个诉求落到实处，而只能诉诸分叉这样无奈而又笨拙的手段。“链圈”对可运维性的诉求来源于传统金融机构使用者对合规性发自本能的自觉遵守，但并没有形成一个完整的技术体系和技术方法论。

首先，“我的资产我做主”绝不是一个与现行法律体系完全兼容的做法。如果在技术上把“我的资产我做主”做实，“做主”在技术上体现为“掌握私钥”，那么在一些场合下，执法措施就落不到实处，就必须事实上迁就区块链的技术设定。在需要进行应急处置的场景，尤其是需要对涉及资产余额的错账、乌龙指、非法所得、不当得利等进行冲正、追究、查封、充公等操作时，这样的做法在法律上有明显的缺陷。所以，从区块链底层把执法措施支持到位是区块链应用单位满足合规要求的起码要求。如果说在之前以借鉴为主的阶段大家还顾不上法律合规性，那么当区块链进入以技术上自主创新、自主掌控为主，应用上以合规发展、为我所用为主的阶段时，这样的要求再得不到满足就说不过去了。

其次，可运维性的要求应该非常清晰地传导到开发方。一是在开发方中逐渐形成基于最佳实践的模板，把有共性的可运维性的功能（比如应急处置特权下的冲正机制、冻结机制、刹车机制以及在线升级机制等）作为模板的标配代码嵌入其中。二是在开发方中逐渐形成基于业内风控理念和通过历史教训积累下来的业务流程参考约束标准，把重要的业务步骤之间共性的合理顺序固化下来。秉持同样运维理念的开发方应该联合起来，形成共享可运维性模板的联盟。通过这样的做法，让区块链应用少走弯路。2016年，中国分布式总账基础协议联盟（ChinaLedger）发布的《面向中国资本市场应用的分布式总账技术白皮书》中，系统地阐述了如何在智能合约层面支持应急处置的问题。

第三，区块链绝不可以看成一个“数据库”，更遑论“分布式数据库”。将区块链当成数据库使用，就会发现区块链只有创建和读取功能，没有修改和删除功能，就会得出“区块链不如数据库”的错误结论。其实，并不是区块链不如数据库，而是不应该把区块链这样来用。区块链上记录的不应该是业务数据，而应该是操纵业务数据的指令序列或其日志。区块链不是要取代数据库，而是要作为数据库的高可靠性的前置。区块链要求日志不可遗漏、不可篡改，但并不是说数据本身不可改动。把一系列操作依序记录在区块链上，然后到真正的数据库中依序执行这些可留痕、可审计、可追责的正常操作和应急操作，操作的最终结果写在真正的数据库而不是区块链中。一旦数据库发生问题需要回滚，只需从区块链的特定高度进行重演，数据库本身的高可用架构也可因此大大简化。应急处置中如果需要对数据进行冲正，只需通过区块链增加一条冲正的数据操纵指令，这个应急处置行为本身既是需要特权许可的，也是留痕的、可审计的。

第四，通过分叉来修正区块链数据，即使在“币圈”也绝对不是值得提倡的事情。分叉本身意味着账本的分裂，但在多条区块链通过跨链机制互联的场景下，会导致与之跨链互联的账本也跟着分裂。也就是说，当分叉遇到跨链，分叉会把本来在一条区块链内的运维问题传导到另外的区块链中，变成一个全网的运维问题，从而大大增加全网的运维难度。所以，从可运维性的基本理念出发，不应该听任动辄分叉，而应该利用互联互通来反制那些轻率的分叉举动。

第五，有缺陷的区块链应用，特别是

智能合约应用上线，是一件十分危险的事情。它不仅可能影响自身的用户群和业务生态，还可能影响其他的用户群和业务生态。由此看来，当区块链技术和应用发展到一定阶段，对承载重要业务、运作重要资产的区块链实行某种形式的应用准入制，要求应用自带某种形式化验证的过程与结果，具备某种标配的应急处置功能，是十分必要的。

第六，区块链可运维性应该成为区块链正规教育和区块链技术培训的必选内容。只有让可运维性的理念和最佳实践深入人心，把不注重可运维性导致的后果充分揭示出来，才能使区块链技术人才建立关于区块链技术的正确知识结构。这些人到了应用开发第一线，才会更加自觉地为区块链应用扎牢可运维性的篱笆。

总的说来，笔者认为，可运维性是区块链应用中不应被忽视的重要诉求，必须从法律层面、行业最佳实践及标准化层面、用法层面加以引导和约束，使可运维性的诉求贯穿区块链应用的始终。 □