基于区块链智能合约的网络威胁情报共享机制及实现

王　飞
甘肃政法大学　网络空间安全学院　甘肃兰州　730070

摘　要：在开放性极高的网络环境下，人们经常受到多元而复杂的网络威胁。为净化网络环境，就需研究如何实现高效、智能、安全的网络威胁情报共享机制，从而将威胁我国网络安全的信息情报基于高协同性进行合理处理。鉴于区块链技术的创新发展，其点对点的分布式信任管理机制，能够形成对网络情报信息的安全传递，并且在其间发挥其可追溯、防篡改、自维护等特性优势，由此，将区块链智能合约作为网络威胁情报共享机制构建以及运行的载体，成为极具可行性的工作方案。本文着重从区块链智能合约在网络威胁情报共享机制构建中的适用性角度分析，构想了基于区块链智能合约的网络威胁情报共享机制内部流程，并做了关于相关机制实现的进一步思考。

关键词：网络威胁情报；区块链；共享机制

引言：

在网络世界中，网络中的威胁情报信息是不可忽视的存在。这类信息带有随机性、隐蔽性等特点，同时能够形成对网络使用者的恐怖威胁、恶意引导等负面的作用，对国家社会的健康发展也造成威胁。而基于区块链智能合约来构建网络威胁情报共享机制这一思路，则是在我国整体的情报融合共享意识增强的情况下出现的，并且要在充分遵循区块链技术特点，以及与主客体两个维度高度适用的前提下实现。

1　基于区块链智能合约的网络威胁情报共享机制的适用性分析

网络安全威胁情报是对组织和机构产生潜在危害与直接危害的信息集合[1]。在不断加剧的网络安全攻防对抗过程中，攻防双方存在着天然的不对称性，网络安全威胁情报共享利用是一种有效提高防护方响应能力和效果的手段[2]。基于区块链网络，技术人员利用P2P组网技术来架设分布式对等网络，初建点对点的合约基础，继而再引入非对称性加密传输算法，使之作为“安全维护者”在节点间数据传输及访问方面发挥作用。智能合约是通过计算机代码构建合约并予以执行的计算机协议，具有高效性，去信任化，自动履行等优点[3]。在网络数据的存储安全、保密方面，技术人员是在相关网络智能合约构架中设置时间戳，以及搭建链式数据区块结构，这样，其数据就能够可追溯、且不容篡改。而网络威胁情报共享机制的运行环节之一，就是一致地、协同地处理数据。该目的的达成，需要技术人员在智能合约中嵌入共识机制，从而使其能够进行自动化编程，以保障各个节点间数据处理（融合共享）的归口性、规范性。贯穿于情报共享过程的一个关键问题，就是区块节点主体间能够形成信任关系，以及协同关系。如果区块链智能合约能够解决该问题，那么其在网络威胁情报共享机制形成中的适用性也就可见一斑。

1.1 共享主体适用性分析

从宏观的视角来分析，网络威胁情报共享机制下的主体应当包括国家、地方以及其他各级网络威胁情报机构，政府部门，社会组织，企业组织，普通群众等。可见，相关共享机制的架设中，对多元化主体关系的融通要求甚高，其所对应的融通，既有国家各级各类部门间的情报资产融合共享，又涉及到纵向的由国家层面下沉至人民群众层面的情报资产融合共享。其中，协同机制以及信任机制，将是情报资产得以融合共享的主要推手。但是，各类型情报共享主体的特点不一，认知也有差异，想要规避主观竞争关系而建立纯粹的信任和协同机制，并不能依靠常规的制度建立、口头约束、法律法规等方式来实现。这时，区块链智能合约就有了用武之地。该技术能够满足相关机制的高信任性、高速率、扁平化要

基金项目：甘肃省科技计划项目（技术创新引导计划）：基于区块链智能合约的网络威胁情报共享机制及实现（20CX9ZA072）；甘肃省高等学校创新能力提升项目：基于区块链技术的网络谣言治理研究（2020A-093）；2018年甘肃政法学院校级科研资助重点项目：基于语义统计分析的网络舆情挖掘技术研究（GZF2018XZDLW20）

作者简介：王飞（1978.07），男，汉族，辽宁阜新人，硕士，甘肃政法大学网络空间安全学院副教授，主要从事网络舆情、区块链方向研究。

求，为情报资产的传输搭设网络链路。

区块链智能合约运用中，各参与节点的主观缺乏信任状态能够被打破。其基于P2P组网以及非对称性加密传输机制，并不受主观意志的干扰，直接由点到点，使得共享主体间的信息壁垒被击破，实现信息融通。简单来说，该技术下的融合共享情报体系，将情报传递的层级简化了，继而也就减少了相关情报受到篡改、损坏的机会，从而使情报资产安全、传输效率均有保证。可见，区块链智能合约能够适用于网络威胁情报共享机制下的复杂主体。

1.2共享客体适用性分析

网络威胁情报共享机制下的客体，即被不同共享主体所传输、汇集、分析的各类情报产品、信息等，它们共同构成了情报资产。这些客体在共享机制运行过程中，以数据形式存在，规范性强，保密度高。能够作为网络威胁情报的数据信息，一般与国家安全问题、民生发展问题等关联甚密。所以，客体被传输中，需要得到高度机密性地保护，例如，相互共享信息的主体应当被设置权限，从而根据权限大小来进行信息检索、分享等操作；情报资产应当统一划归到一个规范而严密的大数据库中，形成长久性地存储机制，并获得高级别维护，从而使这些资产信息作为基于情报共享机制的主体间互联互通的基础。此外，网络威胁情报共享机制下的客体资源来自于多渠道，而且经过了反复地价值验证，其可用性应当得到挖掘。由此，网络威胁情报共享机制也应当能够对客体进行深度挖掘。

区块链智能合约中，嵌入了非对称性加密技术，能够很好地对传输状态下的情报客体进行加密保护。其中，合约公钥将作为区分不同主体的权限的依据，持有公钥者（节点），即可顺利解析情报原始数据。这就实现了对客体资源的保密传输。同时，在智能合约程序中，技术人员还可以进一步进行节点权限、功能的设置，使不同节点的获取、传输情报数据的格式也不同，从而提高了情报资产的归口性。此外，合约中链式数据区块结构的应用，以及共识机制、Merkle哈希树验证机制的应用，也使情报客体的有效性、完整性得到进一步保障。可见，区块链智能合约对数据资产管理的流程能够契合于情报客体的特性的保持。

2 基于区块链智能合约的网络威胁情报共享机制内部流程

相应网络威胁情报共享机制流程形成之前，各合约节点应当统一进行情报共享业务的需求分析，继而以需求为依据进行流程制定，并在合约脚本中融入网络威胁情报融合共享的策略，由此，一个规范化的、可用性强的网络威胁情报共享机制才能得以实现。其相应的流程设计构想如下：

其一，区块链智能合约节点结合网络威胁情报相关业务的个性化需求进行情报资产收集、整合的指标设定，包括明确数据类型、属性，以及时空条件等。

其二，以所收集的数据指标为依据，确定各个参与节点，即情报主体的范围。节点还可细分为管理角色节点、普通角色节点。此外，各参与节点需要得到任务划分，明确自己的分工，例如，界定出由哪些节点负责情报信息的整合、研判，由哪些节点负责执行行动指令和保持协同。这也是形成后续的情报融合共享策略的前提，也能够指导相应策略在智能合约中的脚本部署。

其三，遵循所订立的智能合约规则，形成各参与节点的网络威胁情报融合关系，统一指令，统筹管理。这一步是要实现自动化进行当地数据库关联性资源的收集、检索，并且加密相应的元数据，继而将元数据上传于智能合约。

其四，各个管理节点遵循合约规则，负责将各普通节点所提供的情报共享节点列表、加密元数据、节点ID等概要信息封装于区块链中，封装形式为数据区块。

其五，各个共享节点以数据区块的概要信息为参照，进一步进行加密元数据获取，并且可进行数据认证交互，得到加密公钥。这样，节点主体就能顺利展开对关联数据的解析操作，也即完成了对网络威胁情报的共享。

其六，各主体以智能合约交易规则为参照，将网络威胁情报信息的数据提供节点、加密元数据摘要、共享时间等信息做出封装处理，即将其以交易区块的形式存储于网络威胁情报交易链中。

其七，共享机制内各节点以智能合约规则、情报共享策略为根据，进一步挖掘节点共享的关联数据，包括做出数据收集、分类、研判等，从而将数据转化为可用性的高质量网络威胁情报产品，以及继续以上共享循环。

3 关于进一步确保网络威胁情报共享机制实现的思考

其一，智能合约各节点应当梳理自身业务需求，合理将需求转化为融合共享策略，从而能够在不同网络威胁情报共享任务场景下按规则部署智能合约。这也有利于网络威胁情报资产的广泛性、全链条流动，突出其在当代社会的融合共享应用价值。

其二，各参与节点应该遵循智能合约规则，做好数据采集工作，包括要自动收集、识别数据，在本地数据库关联数据中合理抽取数据等，继而将数据封装、上传至区块链。这能够极大地减少网络威胁情报共享机制运行的成本，提高机制润滑度。

其三，智能合约下的各个共享机制主体，应当同时担当好智能合约发起者和参与者的角色，发挥在指令协同、情报融合、情报共享等方面的积极作用。

其四，随着计算机和网络技术的快速发展，网络安全事件频发，安全漏洞不断，威胁情报的作用和价值越来越大[4]。因此，要在基于区块链智能合约的网络威胁情报共享机制健康运行的基础上，落实好情报数据深度挖掘工作，并且注意其多元化应用场景，以及广泛应用价值的开辟。

4 结语

综上所述，网络威胁情报的共享机制建立，有其必要性，同时也具有可行性。在区块链技术得到跨越式发展的今天，基于区块链智能合约的网络威胁情报共享机制的实现有了更多的技术支撑条件。人们需充分把握其机制设计中的主客体特点，继而合理进行以区块链技术为基础的相关功能要求的实现。此外，网络威胁情报的共享机制建立是要使相关网络威胁情报数据得到挖掘、利用，从而建立起网络安全屏障，因此，相关共享机制运行中，应充分重视该层面功能的实现。

参考文献：

[1]林玥，刘鹏，王鹤，等.网络安全威胁情报共享与交换研究综述[J].计算机研究与发展，2020，57（10）：14.

[2]黄克振，连一峰，冯登国，等.基于区块链的网络安全威胁情报共享模型[J].计算机研究与发展，2020，57（4）：11.

[3]杨磊，马育红，王玉杰.区块链智能合约的利弊分析[J].发展，2020（1）：2.

[4]程叶霞，付俊，陈东，等.基于区块链的威胁情报共享及评级技术研究[J].信息通信技术与政策，2020（2）：6.