

区块链技术在互联网安全中的应用研究

罗珍

中共西藏自治区委员会网络安全和信息化委员会办公室 西藏 拉萨 850000

[摘要]随着现代网络科技的发展与网络用户人数的增加,互联网空间安全管理问题日益凸显,为捍卫我国网络主权,解决各类网络安全问题,有关部门与企业管理者必须合理运用区块链技术,搭建分布式信息传输系统,对重要信息进行加密与远程存储处理,把握现代分布式科技和网络安全之间的密切关系,提升网络空间的安全性,拓展区块链技术应用路径,使得各机构从不同节点获取不可更改、经过标准化认证的信息。本文主要分析了我国现代区块链技术的核心原理与基本特性,并指出了现代网络空间安全管理制度的缺陷与面临的主要挑战,总结了在互联网安全管理中合理运用区块链技术的必要性与可行路径。

[关键词]信息科技;区块链技术;互联网;安全管理

【DOI】10.12252/j.issn.2096-6261.2021.09.1982

区块链系统是具备开放性、层次性的共享数据库,其核心架构、整体功能克服了传统单中心网络服务体系的缺陷与不足,可支持节点所有者变更信息存储方式与数据传输渠道,全面展现其所具备的内部稳定性与安全性。区块链系统支持管理者对存储在服务器中的数据进行认证加密与验证,发现并剔除其中的虚假信息,有效抵御病毒与非法网络信号的攻击,弥补现有网络安全防护体系的缺陷。

1. 区块链技术的基本原理分析

区块链是一种将数字化信息基于时间顺序赋予标识,将其以链路的形式组织在一起,形成一种复合型、可调节的加密数据形态,此类数据形态具备可变性、可追溯性,是基于现代化数据库技术与远程链路传输技术构建的新科技。区块链技术具备去中心化、在线传输、加密认证等基本特点,可由多个中心、不同节点传输并存储核心数据,让所有联网设备均承担起复刻数据、记录链路标识的任务,在某一个节点或数据中心失效后,其他服务能力较强的节点会承担起数据传输、存储任务,因此一旦数据或信息被记录到区块链中并上传至多个服务器内,则信息将永远无法被单方面修改、删除,此类技术所具备的特殊分布结构有利于保存行业机密与重要信息,能够使得信息的使用者、发布者脱离某一固定信息传播中心的影响与控制,可支持参与者进行匿名、远程的信息交换与在线商业交易,处于不同地区的区块链使用者能够在杜绝私自更改信息的前提下,基于共识机制交换真实数据。区块链的用途较为广泛,相对与传统的点对点数据传输机制与加密算法而言,具备更为突出的稳定性与安全性,其输出结果是否符合内部规则取决于某一链路服务器所提交数据的真实性,一旦数据被人为地单方面修改,则会自动触发响应机制,输出错误结果,这一错误结果可被其他服务器上的信息使用者所识别,引发系统内部环境的变化^[1]。

2. 我国互联网安全管理制度面临的危机与挑战分析

步入网络时代以来,计算机用户开始大量使用数据容量较大、携带方便的移动存储设备与数字化云端存取服务,

现代化办公设备可支持在线数据传输与文件备份,但现代化网络空间中充斥着带有一定危险性的虚假信息与包含带有感染性计算机病毒的网页,给存储于计算机中的信息带来了不安全性,信息容易在日常生活中丢失或被不法分子修改、复制,相关违法行为给人民群众带来了较大的经济损失,影响了大众对网络空间的信任。2010年以来,我国国内网络安全问题层出不穷,多家著名企业内部云端服务器遭到不法分子入侵,各类用户专有文件与企业内部机密丢失,目前我国网络服务商与企业常用的网络安全管理制度较为落后,依然沿用传统的一元化、中心化数据管理体系,其抗风险能力较差,网关密码容易被黑客与内部人员破解,管理用户的权限过于集中,无法及时排除潜在的安全隐患,反而使得不法分子入侵服务器的难度有所下降。黑客可通过首先破解高权限账户的密码与认证机制,登入服务器,并根据自身需求修改、复制、清除存储在服务器内的各类数据与机密电子化文件,引发一系列危害性巨大的安全事件^[2]。

3. 区块链技术在互联网安全管理领域的应用价值研究

3.1 发现侵权与违法行为,维护网络环境安全性

区块链技术所采用的在线认证安全体系能够促使不同地区的服务用户形成内部共识,借助来自多台服务器的运算能力,验证某一节点所上传的文件块内容是否正确,以独一无二的数字序列对数据内容进行检测,为通过认证的数据赋予全新编号,去除不实、虚假、蕴含病毒的错误文件,进一步净化网络环境,维护网络空间的安全与稳定^[3]。在这一全新的数据传输体系中,多数节点可团结一致,针对不法分子主导的上传虚假数据行为进行反击,同步上传经过共同认证的正确数据与不可复制的验证信息,杜绝可能出现的私自修改信息、偷窃用户个人信息等行为,有利于构建一个开放、稳固的网络安全共同体。

3.2 满足网络安全需求,促进安全技术融合

区块链技术的普及应用,可进一步促进多种类型网络安全防护技术的融合与同步应用,此类技术具备较为突出的防

伪能力，可与防火墙、序号认证等安全技术进行深度融合，突出安全防护功能的多样性、合理性等基本属性。例如在网络安全管理人员审计主机账号与服务机制的同时，区块链服务器管理者可根据自身需求，对带有明确认证信息的网络主机、通信设备进行登记，为其打上独特标识，将相关数据传输到多个节点，以此提升数据库内部信息的审计速度，保证审计活动的精确性、有效性，节点管理者可选择采用旁路接入模式，对存入数据库的信息进行评估、检测，搭建虚拟化的网络安全管理平台与数据筛选机制，促进不同领域、不同行业数据的互通与相互转化，并保证用户个人隐私与企业内部数据的安全性、机密性。

4. 区块链技术在互联网安全管理中的正确应用路径

4.1 在线资产管理与信息传输交流

通过合理运用区块链技术、搭建远程多节点信息传输系统，资产持有者可对自身所拥有的无形资产、有形资产进行持续性监控，对其使用方式、传播路径、变现渠道进行规划与探索，保护自身知识产权与资产使用权，避免不法分子伪造、修改自身所持有的数字化资产，并就自身所持有的排他性资产所有权在线上和其他区块链系统使用者进行交易。区块链系统可赋予不同类型的专有资产以可追溯、可认证的资产所有者标识，可快速清除数字化交易市场上流通的假冒伪劣产品，对用户持有的无形资产进行有效管理，可支持给无形或有形资产建立独特的数字化档案与所有权证书，记录各类信息与资讯的出处、来源、主题，为不同类型产品的商品交易流程提供可追溯的信息，支持资产所有者与交易者进行在线源头认证服务，查询此类数字化资产的生产时间、配置、基本功能、用途等各类信息，提升虚拟资产的使用价值与安全性，区块链所具备的安全保护性能，获得了不同领域的一致认同，通过将在线认证机制、评论机制引入区块链系统，可满足多数网络用户的固有需求，可支持网络社区用户实现内部资产交易。

技术人员可在物联网领域引入区块链认证技术与分布式信息传输系统，顺应时代发展趋势，将多种类型的资产接入互联网，例如在汽车、房屋、艺术品上安装传感器与信息感应装置，并将其连接到区块链的节点与服务器中，结合移动互联网技术与移动智能科技，发挥区块链系统固有的优势，即运算能力强、稳定性高等，解决物联网系统潜在的安全问题或信息加密困难问题，满足用户基础设备连接网络、获得实时认证信息的特殊需求，利用区块链系统所具备的分布式架构与自动化认证机制，使之支持更多数量的移动设备与智能化可操控终端，利用非对称加密、分布式计算技术，为资产所有者安全使用连接到物联网上的个人资产、工具提供便

利性，提升不同位置节点之间的信息传输、交换速度。

4.2 隔绝分布式服务攻击，提升服务器稳定性

我国网络空间中DNS服务器经常受到不法分子所组织的在线干扰与攻击，黑客习惯于采取固定模式，向网站中的DNS服务器发送数量较大、无法快速处理完成的服务请求，在短时间内挤占多个信息交换渠道，使得正常用户的可用信道资源与网络资源大量减少，DNS服务器因拥堵而造成网站停止运作或服务器宕机，引发大规模的网络空间崩溃。目前一体化、单个中心的网络架构容易受到黑客的攻击，部分承担数据传输任务的节点具备脆弱性，存在无法控制的安全风险^[4]。区块链技术可拓展节点数量与信息传输渠道的容量，为网站或信息中心提供高质量的多节点同步数据传输服务，并进行快速的域名解析，发现来自未认证网站或节点的错误数据并加以屏蔽，管理者可建立配套的白名单制度，杜绝不法分子的网络攻击，提升网络信道资源的利用效率，使得未受到攻击的网络节点承担起传输数据、提交用户请求的任务，有效抵御可能出现的DDoS攻击，用户与服务器之间可建立信任，通过白名单制度登记可靠用户，封闭未经认证的特殊域名与网站，调整设备连接方式。

结语

区块链技术具备独立性、自治性，能够在开放性的网络空间中持续稳定运行，排除潜在的安全风险与中心化隐患，让不同地点的用户在高度互信前提下进行在线交易，为节点之间的数据传输创造一个稳定、安全的环境，有效防控具备较大危害性的网络攻击与恶意行为。网络安全管理者可使用区块链技术，将其用于保护数据中心存储的各类信息，把握该技术的优点与缺陷，做好节点信息备份与资产认证管理，拓展其基本功能，使之和其他类型的网络安全技术结合，基于共识机制预防攻击、清除不正确的错误数据，汇聚来自不同领域的系统信息并进行加密、备份处理，有意识地促进区块链系统的正确应用与不断发展。

参考文献

- [1] 李枕恬, 郭翔宇, 宁黄江, 等. 区块链技术在工业互联网中的应用及网络安全风险分析[J]. 工业技术创新, 2021, 08(02): 37-42.
- [2] 陈要伟. 区块链在物联网安全中的应用研究[J]. 产业与科技论坛, 2020, 19(22): 57-58.
- [3] 汪焱. 区块链技术在互联网安全中的应用探究[J]. 企业科技与发展, 2019(02): 133-134.
- [4] 李宪萍, 杨赫. 浅析互联网信息安全中区块链技术的创新与发展[J]. 科学与信息化, 2021(3): 58.