文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于区块链技术的数据安全与隐私保护机制

----以信息管理与信息系统中的数据与隐私为例进行研究

刘涛
华为云计算技术有限公司
DOI:10.12238/acair.v2i2.7400

[摘　要] 随着信息技术的发展,数据的收集和存储使用技术变得越来越完善。巨量的信息对数据安全与隐私保护机制提出了挑战,为了满足数据安全保护的现实需求,更新隐私保护机制变得越来越迫切。本文从区块链技术入手,阐述了信息管理与信息系统中基于区块链技术的数据安全与隐私保护机制研究。
[关键词] 区块链技术；数据安全；隐私保护
中图分类号：TP309.2　文献标识码：A

Data security and privacy protection mechanism based on blockchain technology

----Take the data and privacy in information management and information system as an example

Tao Liu
Huawei Cloud Computing Technology Co., Ltd

[Abstract] With the development of information technology, the collection, storage and use of data technology has become more and more perfect. The huge amount of information poses challenges to the data security and privacy protection mechanism. In order to meet the realistic needs of data security and protection, it becomes more and more urgent to update the privacy protection mechanism. Starting with blockchain technology, this paper expounds the research on data security and privacy protection mechanism based on blockchain technology in information management and information system.
[Key words] blockchain technology; data security; privacy protection

前言

随着信息技术的发展,保护个人隐私数据变得越来越迫切。旧有的隐私保护方式在信息技术发展的冲击下,存在着数据泄露等风险。区块链技术作为一种新兴的技术形式,在保护个人隐私数据上大有可为。人们可以更加深入地研究探索区块链技术,以此保护个人隐私安全。

1 区块链技术概述

区块链技术是一种被作为比特币的底层技术而进行研究的,去中心化的分布式账本技术。[1]区块链技术之所以以此为名,是因为该技术可以将数据记录成一系列不断增长的区块,这些区块通过特定的方法不断地连接到一起,从而组成一个不可篡改的链条。这种技术进行开发的原因就是可以适用于多个领域。因此,区块链技术在网络数据安全领域也大有可为。

区块链作为一种以分布式网络为表现形式的技术,它所应用的数据存储方式,并不是将数据存储在集中的服务器当中,而是将数据分散地存储在多个节点上。该特点就决定了a块链技术没有单一的控制中心,由多个节点进行数据维护和数据验证的特征是区块链技术降低了单点故障的风险。

除了规避数据单点故障的风险之外,区块链技术还有很多优点。传统的数据安全隐私保护技术中,数据很容易被篡改。但是,区块链技术的特点和机制就决定了,一旦数据被写入区块链,就很难被进行修改。篡改区块链技术中所存储的数据信息是十分困难的,这一特点就保证了用区块链技术所保存的数据的完整性和真实性。区块链在保证数据不被篡改的同时,其所记录的数据也是公开可查的。技术的使用者可以通过查看其上所有的历史记录来确保数据操作的可信程度,这种透明度也使得数据变更更容易被查询和追溯。当该技术所记录的数据出现一点改动时,会变得十分清晰可见。区块链技术还应用密码学来保护数据的隐私。[2]这就为数据的访问设置了一定的门槛,只有拥有密钥的人才可以访问应用该技术所储存的数据,提高了数据的安全性。

2 数据安全与隐私保护面临的困境

2.1互联网带来的安全隐患

互联网给人们带来极大便利的同时，也对人们数据安全与隐私保护带来了极大的挑战。互联网作为一个较为开放的平台具有匿名性的特征。当用户使用互联网时使用虚假身份，那其在互联网上的行为就变得难以追溯和控制，为网络安全造成了一定程度上的安全隐患。互联网的特殊结构使得其储存数据的服务器很容易受到不怀好意的人发起的攻击，容易对互联网的数据安全造成威胁。互联网联通了各个国家各个地区的信息网络，网络上的攻击和威胁也容易波及的范围很广，例如网络攻击可以跨越国度。但是在实际的管理过程当中，由于国家主权等综合因素的影响，很难进行跨国审判。

2.2国际标准不统一

尽管网络技术可以联通各个国家的使用者。但是，不同国家在网络安全方面所制定的法律法规并不相同，不同地域遵循着不同地域的网络安全规定。这种各自为政的前提下，导致很多跨国企业和组织或者网民在进行交流时，很难有统一的网络安全规范标准来规范他们的行为。特别是面对跨境数据交流方面，需要各国合作进行应对。[3]全球网络安全规范标准不一致，极大地削弱了网络安全防控的能力，增加了网络安全风险。

2.3人工智能所带来的风险

随着网络科技的发展，人工智能的出现降低了一些网络犯罪的成本。人工智能的语言模型，在经过一定的训练和学习后，可以学习程序编写。初通网络技术的网络新手通过人工智能的帮助，也可以编写出一些恶意程序。犯罪成本的降低，容易让一些用户突破道德底线，对数据安全与隐私保护造成威胁。

3 区块链技术应用于数据安全及隐私保护机制的优势

3.1加强对底层网络的安全防护

互联网的特点就决定了，如果互联网底层网络受到攻击和威胁，容易在连锁反应下导致整个网络的崩坏，对社会秩序产生巨大的负面影响。当某一区域网络受到黑客攻击，导致服务器受损时，与该区域网络进行连接的所有网络系统都会受到影响。区块链技术与传统技术不同，可以加强对互联网底层网络基础设施的保护。[4]区块链技术可以通过确保数据的完整性，实时对数据进行监测以便及时作出应对，通过提高网络系统的透明性来增强网络系统的安全性。区块链技术以维护底层网络的安全和稳定，为网络数据的安全提供了有力支持。

3.2加强对网络数据的维护

应用区块链技术的网络数据具有不可篡改的特点，该特点保证了数据的完整性和真实性。区块链技术中，每个区块都包含了前一个区块的哈希值。当有人恶意想要篡改其中一个部分的网络数据时，会导致整个区块链的哈希值发生变化，可以让人们及时发现网络数据被篡改，从而做出防护和补救。区块链的可追溯性和公开透明的数据查询方式，保证了数据流动的安全。区块链技术的机制也提高了网络服务器的抗攻击能力。

3.3增加通信环境的安全性

区块链技术还可以提高网络通信技术的安全性。传统的网络信息技术，很容易牵一发而动全身，某E网络节点出现问题时，会影响到整个网络的安全和运行。区块链技术在提高数据信息传播效率的同时，也保证了整个网络环境的稳定。在某一网络节点出现问题时，区块链技术保证大部分的节点都可以继续工作。应用区块链技术可以创造出一个更加安全，更加完善的通信环境。

4 区块链技术应用于数据安全治理的困境

区块链技术固然相较于传统技术，传输信息方面更加高效。但是对于该技术，如果运用不当，仍然会破坏网络环境的稳定，不利于数据安全治理。区块链技术的复杂性和匿名性，不利于相关监管部门的监管，不利于犯罪嫌疑人的追踪和抓捕。国际社会也缺乏相关管理规范，当各国企业和组织跨国进行合作时，很难进行行政和司法上的协作，不利于治理跨国网络犯罪行为。

区块链技术使用不当也很容易为网络安全环境造成巨大威胁。区块链的去中极化和隐匿性特征，就导致了，如果该技术被滥用很容易对网络安全也造成很大隐患。“暗网”便是该技术的产物，该平台难以追踪并监管，造成了大量数据的泄露和滥用，成为不法分子的工具。因此，区块链技术不当使用也容易造成很大的网络风险，甚至有可能对网络运行的秩序造成极大威胁。

5 基于区域链技术的数据安全与隐私保护机制探索

5.1形成多元协作共治机制

多元主体、多元机制是完善网络数据安全治理体系的主要内容。开展有关数据安全知识的宣传普及，增强全社会的网络安全意识，国家、企业、机构、个人等多方共同参与到保护网络数据安全当中来，才能够营造一个良好的网络环境。因此，应当在国家统筹之下，在多方主体的共同努力下，建立一个更加完善的网络数据安全治理制度。政府要发挥好其监管和协调作用，监督社会各部门的工作效率和资源分配的合理程度，推动各部门的互相协作，从而解决网络相关问题。这样的统一协作可以大幅度降低使用区块链技术所带来的相关风险。加强机构和组织间的相互合作，整合有效资源提高工作效率，促进网络技术不断更新发展。企业和个人也应当起到一定的监督作用，不断提高自身的知识储备和专业技能，围绕网络技术发挥自身技术监督安全评估的作用。

5.2制定国际标准

当前，网络技术的飞速发展促进了各国产能提升。各个国家都极其重视网络安全技术的研究。技术的飞速发展会导致技术标准不断地进行更新迭代，应当掌握技术标准的发展，引领信息技术未来发展走向，掌握国际标准制定的话语权，才能更好地反映发展中国家发展的利益需求。自从我国践行网络强国战略以来，一直运用多种手段和途径参与到国际网络数据安全治理当中来。我国在国际网络安全治理当中的话语权和影响力也变得越来越高。[5]为了维持国际网络数据安全治理健康平衡的环境，应当加强对于区块链技术等新兴技术的研发投入，不断提高我国在网络数据安全治理当中的影响力。

5.3构建国家主权区块链制度

为了更好在网络数据安全治理的环节当中维护政府权威，降低技术所带来的风险，应当树立国家主权区块链概念，以此来更快更安全地促进区块链技术的发展。国家主权区块链与普通区块链不同，更加强调国家主权有着更强的监管性，当网络置于法律监管之下，以此来治理的网络更具安全性。除此之外，由于区块链技术还具备不可篡改的特征，如果有人非法上传虚假数据容易产生共谋风险。因此，国家应当重视相关数据审查，建立相应数据合规审查制度，发布区块链监管规范和行业标准，建立私有链接备案审查制度。当主体端被上传违规数据时，应当按照相应技术标准和法律法规来进行审查治理，以此来实现数据安全及个人隐私保护的现代化和规范化。

6 结束语

区块链技术作为一种新兴的信息网络技术，其使用有利也有弊。该技术可以广泛应用于网络治理、政务服务、社会治理等方面，提高网络运行的工作效率并提高网络的安全性。从另一方面来讲，应用技术也应当具备相应的监管手段。为了更好地进行网络安全治理，建立多元协作共治机制十分重要。国家应当大力发展信息技术引领国标标准制定，努力提高中国话语权，摆脱被动局面。做到数据安全和隐私保护有法可依，由此才能促进网络技术的健康发展。

[参考文献]

[1]王皓阳.基于区块链技术的网络数据安全治理探究[J].网络空间安全,2024,15(01):113-117.

[2]徐军,姜奎,张宗宇,等.大数据背景下基于区块链技术的高校网络信息安全模式研究[J].湖北第二师范学院学报,2023,40(02):5-10.

[3]何黎明,周剑涛,张静.基于区块链的网络数据安全主动防御系统设计[J].技术与市场,2023,30(11):89-91.

[4]武杰.基于区块链技术的网络隐私数据安全防护模型设计[J].中国信息化,2024,(01):73-74.

[5]王越.基于区块链的网络数据安全主动防御系统设计[J].网络安全和信息化,2024,(03):43-45.

作者简介：

刘涛(1983--),男,汉族,陕西富平县人,本科,主任工程师,研究方向：信息管理和信息系统。