

# 区块链技术在网络安全建设中的研究

梁泽潘

(广州市技师学院, 广东 广州 510440)

**摘要:** 当前, 互联网技术的辐射范围越来越广, 人们对于数据的计算与存储安全性要求更高了, 更使得区块链技术下的网络安全建设工作日渐紧张, 安全性成为广大互联网从业人员应当遵守的职业道德和职业底线。本文对区块链及区块链技术进行了简单定义, 进而延伸至其特性, 再就区块链技术在网络安全建设中的运用策略展开了详细叙述, 希望能够为区块链技术在网络安全建设中的应用贡献力量。

**关键词:** 区块链技术; 网络安全; 建设策略

DOI: 10.12373/xdhjy.2022.02.4492

时下, 区块链技术的应用十分火热, 人类也早已从以物换物的交易模式中挣脱出来, 逐渐发明出货币, 第三方“中介”更是应运而生。经过长久的历练和考验, 区块链技术在网络安全建设中的应用是可行且高效的, 网络信息安全防护所涉及的领域各式各样, 恰所需的约束与制度更是应当综合统筹、尽善尽美。相关技术人员也只有掌握了网络安全需求动态, 才能够从多个方面进行安全防护, 真正将区块链技术的积极作用展示出来。因此, 关于区块链在网络安全建设中的应用研究具有十分重要的意义。

## 一、区块链技术的定义

区块链技术是指运用某种方式将数据块连接起来, 每一个数据模块之间相互连接形成数据网络, 从而能够进一步实现数据共享。当我们将区块链看作一个整体时, 它具有的数据存储与数据共享等都能够展示出独特的功能与价值, 相较于传统的信息存储方式已然日新月异了。基于此, 我们可以将区块链技术看作是一种独具多样化数据存储和信息处理的方法。

## 二、区块链技术的特性

### (一) 开放性

区块链系统具有开放性, 其中存储的大部分数据都是可对外公开的, 用户也能够顺利地通过端口访问数据, 进而查询数据、浏览信息, 甚至可以完成下载。但其中存在一小部分数据涉及整个系统的安全性, 只有通过加密的方式进行数据保护, 使得没有权限的用户无法进入该页面获取数据, 使得这一部分加密数据处于保密状态。

### (二) 自治性

区块链技术与传统网络安全技术不尽相同, 在原理、特性、优势、应用等方面更是尽显不同。区块链系统中信任的对象不是特定的, 更不是指定的用户或网络管理员, 而是具有结构性的网络系统。这一系统支持下的人为因素无法对数据实施干扰, 更不似传统网络安全技术一样削弱了大部分参与者的权限和能量, 从而使得“人”的干预更少了, 系统的复杂性也远远提升了, 从而带来了更加安全、高效的保障。区块链技术中, 系统的相关协议规定了具体事项, 也就是说数据的安全性有了根本保障, 各个节点也需要在特定的权限空间下完成数据交换。这是区块链技术取得的突破性进展, 更是数据交换时衍生出的数据系统自治性。

### (三) 匿名性

区块链技术中隐含的加密技术呈现出非对称性, 更使得系统在正常运行条件下, 各个节点之间能够达成协议共识, 从而使得数据交换场景发生在匿名条件下。这样一来, 数据交换有了隐私性, 加密技术的应用再一次为数据安全性提供了根本保障。

### (四) 不可任意变动性

不可变动性在区块链技术的应用过程中十分明显, 用户将数据信息存储在区块链系统中, 这些数据不会被任何人为因素或系统因素修改, 相应的权限更是不会轻易对外开放, 因而能够为数据信息提供安全性保障。而当用户自身想要人为修改其中的数据信息时, 他们就必须通过申请流程获得权限, 才能够一步步通过系统的协议, 进而在节点安全防护级别之内完成相关权限下的修改服务, 不论是数据修改、数据添加、数据删除等也都是在安全条件下完成的具体操作。

## 三、区块链的安全性

### (一) 数据使用安全

数据使用安全是基于节点安全条件下的, 更是去中心化管理体系下数据在系统内外形成的有效对接。在权限分离的情况下, 当我们想要去提取相关信息时, 这一系统带来的便利性不容忽视, 同时也能够降低中央机构安全风险的发生概率。侧面来看, 这也归功于区块链系统的安全性能极高, 使得区块内的信息很难被人为干预, 更进一步提高了数据使用的安全性, 在极大程度上避免了数据使用的风险性。当系统程序访问数据时, 用户也能够第一时间收到是否获取权限的信息, 使得用户的真实感与体验感更强了, 他们也能够主动地参与到维护数据安全过程中来。前文说到更改数据的复杂流程与安全条件, 那么区块链系统对于存储数据的加密技术、权限设置、节点访问、提交分析等再一次提高了防护级别, 用户想要再次更改数据之时就需要重新更新权限设置, 确定区块链中存储的原始条件仍然处于权限设置状态, 下一步节点收到访问请求, 等待权限审核通过后便可再一次访问数据。这一过程中, 系统与节点中的申请与访问记录能够保存下来, 节点的效用也产生于更改后的权限设置, 其溯源性又是一层安全防护网。在此基础上, 用户能够一次次进入系统中修改权限设置, 他们的行为也将被记录下来, 系统中具备相应权限的用户都能够

对访问记录进行审计。总之，区块链技术在数据使用安全性上十分明显，这既是其特性，更是其在使用过程中能够展现出的优势。

## （二）系统安全性

区块链系统在设计之初就需要对区块链进行编码，但其编码又容易出现漏洞，进而导致一些不良手段造成的网络攻击、病毒攻击等。这样一来，便可能对整个区块链系统造成损害，从而导致整个系统的正常运行受到影响。但对于区块链技术来说，每一节点又都具有独立性，尽管病毒攻击的是大范围节点，仍然能够保证一部分节点的正常运行和数据传输，从而保证了整个系统的安全性。基于此，区块链作用下的网络安全建设工作十分高效，也能够为用户创建一个相对完全的网络环境，既能够为用户提供更加优质的安全服务，又能够维护系统的安全性。

## 四、区块链技术在网络安全建设中的应用

### （一）网络数据完整性方面

传统网络安全技术应用过程中，边界防护系统将对网络数据进行安全保护，这是通过数据加密来完成网络安全防护的。区块链技术的应用能够在此基础上优化和提升，从而有助于解决传统网络安全技术中存在漏洞和隐患问题，保证网络安全建设工作的有序进行。为进一步提高网络的安全性，引进新的理念和创新技术必不可少，也就是说必须要对安全技术进行革新与调整。区块链技术的应用虽与传统网络安全技术有着较大的差别，但是需要对区域内部所有网络数据进行监视，从能够提供出最新的数据信息，进而对区块链中的数据进行攻击和防护、控制。

### （二）应用在通信技术方面

区块链技术的应用能够提高网络通信的可靠性，一方面，它能够在短时间内将数据信息传播到世界各地的网络节点上，从而让数据信息快速、高效地蔓延开来，成为实现高效性与安全性并存的信息传播载体。另一方面，假使身处于无线网络环境中，或者互联网服务突然中断，区块链技术支持下的高频无线电或者传真手段仍然能够完成信息传递。因此，多样化、复杂化的信息背景下，区块链技术在通信方面的应用依然能够净化网络服务环境，带给广大用户以安心和放心。区块链网络系统中，网络节点无法部署中心化，当一个节点或一部分节点出现故障时，并不会对整个系统造成巨大冲击而导致不可挽回的损失，使得信息仍然能够在网络通道中高效传递。再不济大部分网络节点被攻击或者损害时，剩下的部分节点仍然可以正常运行；或是区块链系统受到病毒攻击，其内置的协议方式也能够保证数据的安全性与可靠性。总之，区块链技术在通信方面的应用十分奏效，更是能够有效保障网络通信的安全性与可靠性。

### （三）网络资产管理中的应用

在有形资产与无形资产方面应用区块链技术也是相当可观的。区块链技术的优势之一是能够对网络资源进行严格的监督与管理，进而保障数据信息的一致性与安全性。应用区块链技术管理网络资产能够对所涉及的域名、知识产权、积分等进行有效、高效的

管理，极大程度上保证了资产的安全性。而在对有形资产的管理方面，区块链技术能够对有形资产进行统一标注与管理，还能够与物联网技术相互配合，共同记录资产转移的信息，进一步实现资产溯源、检查等，从而能够掌握商品的流通过程，助力相关产品经理、产品数据、产品服务越来越透明化、高效化。由此可见，区块链技术的应用能够高效管理好有形资产与无形资产，从而在安全范围内保证其更好的配置和流通。

### （四）应用在社交网络方面

区块链技术应用在社交网络方面能够集成用户评论、投票等功能，进而能够辅助设计出更适应现代网民使用习惯的网络公约。这样的方式不仅仅为用户提供了便利，还能够对用户的网络行为进行监督与规范。与此同时，数字货币的使用也在虚拟环境下更加频繁了，更进一步加强了对社交网络用户的管理。

### （五）网络基础设施中的应用

区块链技术应用在基础设施方面依赖于 DNS 技术，以其提供应用程序服务，但假设 DNS 技术发生故障，将极有可能造成大范围的网络服务中断，进而影响到用户的体验感和真实感。此事借助区块链技术连接系统，可以高效建起网络保护机制，让网络应用处于一个相对稳定的环境下，从而能够减轻网络中断带给用户的不良体验，这是区块链技术在网络基础设施中的应用价值。

## 五、结语

总而言之，区块链技术在网络安全建设中的应用独具优势，也是网络安全防护工作的一大突破与进展。从原理上来看，区块链技术的应用既能够做好任意模块间的交流与沟通，也能够保持故障节点的独立性与隔绝性，从而不会让一个节点的问题影响整个系统的安全性。从特性上来看，区块链技术的应用具有开放性、自治性、匿名性、不可随意变动性、高度安全性等特点，因此在网络安全建设工作各方面的应用能够发挥出最大价值。区块链技术在网络安全建设中的应用既是一次伟大的革新，也是新时代背景下技术革新的重要见证。

## 参考文献：

- [1] 徐恪, 凌思通, 李琦, 吴波, 沈蒙, 张智超, 姚苏, 刘昕, 李琳. 基于区块链的网络安全体系结构与关键技术研究进展 [J]. 计算机学报, 2021, 44 (01): 55-83.
- [2] 杨珂, 玄佳兴, 王焕娟, 李国民, 沈雪晴. 区块链技术在能源电力行业的研究及业务应用综述 [J]. 电力建设, 2020, 41 (11): 1-15.
- [3] 王玉英, 李岩, 李念峰. 基于区块链技术的网络文化信息安全传播机制与路径研究 [J]. 情报科学, 2020, 38 (10): 35-40.
- [4] 杨书惠, 彭博, 广瑞, 李子晗, 陈双梅. 基于区块链技术的网络空间安全机制 [J]. 电子技术与软件工程, 2019 (13): 192.