基于区块链技术的网络空间安全解决方案研究

中国海关传媒中心　赵飞
首都信息发展股份有限公司　郭婷

编者按：探究将区块链技术融入网络空间安全架构，提出综合解决方案，通过构建分布式信任等关键模块，有效提升网络安全性能。

数字化时代，网络空间成为社会经济重要基础设施。然而，网络攻击手段层出不穷，安全事件频发，传统的防火墙、入侵检测系统等防护技术在面对新型威胁时力不从心。区块链技术的去中心化、不可篡改等特性，为解决网络安全问题开辟了新路径，助力构建更安全可信的网络环境。

以区块链重塑网络安全架构

1. 系统架构概述

基于区块链技术的网络空间安全架构致力于搭建一个全方位、多层次的安全防护体系，实现网络空间数据的安全存储、传输与共享，以及对用户身份的可信认证和访问权限的精准把控。该架构（如图1所示）主要涵盖分布式信任网络、数据安全存储与共享模块、身份认证与访问控制模块以及智能合约驱动的安全策略执行模块。各模块协同合作，构成一个有机整体。

分布式信任网络是整个架构的根基，借由区块链的共识机制，保障网络中各节点间信任的建立与维护，摆脱对中心化信任机构的依赖。数据安全存储与共享模块运用区块链的加密技术和分布式存储特性，将数据加密后存储于多个节点，确保数据的完整性和保密性。身份认证与访问控制模块基于区块链的数字身份技术，为每个用户生成独一无二的数字身份标识，并借助智能合约对用户访问权限进行动态管理。智能合约驱动的安全策略执行模块依据预先设定的安全策略，自动执行各类安全操作。

2. 分布式信任网络与智能合约安全策略

分布式信任网络是架构的核心。区块链技术引入工作量证明（PoW）、权益证明（PoS）等去中心化共识机制，让节点无需信任第三方即可达成共

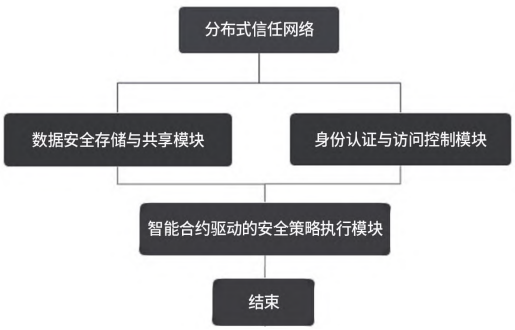

图1　网络安全架构图

识，构建分布式信任关系。

本架构采用改进的权益证明共识机制选举记账节点。设节点综合得分S，节点信誉度R（取值范围 0~1，值越高信誉越好），持有权益E，权重系数分别为α和β（$\alpha+\beta=1$），则综合得分公式为：$S=\alpha R+\beta E$。节点信誉度依据历史行为记录评估，如参与网络维护积极性、遵守安全规则情况等；持有权益体现了对网络的贡献程度。将交易记录和节点行为信息记录在区块链上，形成可追溯账本，便于安全事件时定位问题，追究责任。

智能合约是区块链的关键应用，以代码形式部署在区块链上。基于区块链的网络空间安全架构借助智能合约实现安全策略自动化执行。安全策略以智能合约形式编写并部署在区块链上，涵盖网络攻击检测与防御、数据安全保护、用户行为监控等策略。当满足触发条件时，智能合约自动执行安全策略。例如，设$F>T\times(1+\delta)$，T为正常流量阈值，F为当前流量，δ为可接受流量波动系数。在检测到网络流量异常时，即自动触发防火墙规则来限制异常流量；当发现数据被非法访问时，自动记录日志并通知安全人员。

3. 数据安全与身份管理

基于区块链技术的数据安全存储与共享模块采用加密存储和分布式存储相结合的方式来保障数据安全性和可用性。采用对称加密和非对称加密进行数据加密。加密后的数据被分割为多个数据块，存储在区块链网络多个节点，每个节点仅存储部分数据块，以降低数据被窃取的风险。

在数据共享方面，通过智能合约精细控制访问权限。数据所有者可设置不同用户或用户组的访问权限，如只读、读写、可下载等。当用户请求访问数据时，智能合约依据预先设定的权限规则，设权限规则为权限矩阵P，用户身份标识U，数据资源标识D，当$P(U, D)$为真时，通过验证的用户才能获取数据。区块链的可追溯性保证了访问记录的完整性，便于审计和监管。

身份认证与访问控制是网络安全的重要环节。基于区块链的身份认证与访问控制模块采用去中心化数字身份技术，提供更安全便捷的服务。用户在区块链上具有唯一数字身份标识，由公钥生成，不可篡改且唯一。智能合约根据用户身份、角色和访问策略，自动判断访问权限。当权限变化时，智能合约可实时更新权限信息，确保及时性和准确性。

关键技术实现与测试分析

该方案涵盖了一系列关键技术实现及全面的测试分析，以确保其安全性和性能满足实际需求。下面将从加密算法优化、智能合约开发部署、分布式存储与数据一致性维护，以及搭建测试环境进行安全性和性能测试等方面展开阐述。

1. 区块链加密算法优化与测试

区块链加密技术对于保障数据安全至关重要。本研究对传统加密算法进行优化，采用椭圆曲线加密算法（ECC）作为非对称加密算法，选用高级加密标准（AES）作为对称加密算法。通过改进加密模式和密钥管理方式，提升加密的安全性和抗攻击性。同时，引入同态加密技术，允许在密文上进行特定计算，无需解密数据即可实现数据在加密状态下的安全处理。例如在数据统计分析时，可直接对加密数据进行计算，得到加密结果，仅授权用户能够解密获取最终统计数据，从而有效保护数据隐私。

为验证加密算法优化效果，本文进行了相关测

试。表1是不同加密算法在加密速度、密钥长度、安全性强度方面的对比测试数据。可以看出，优化后的ECC和AES算法在加密速度和安全性强度上均有显著提升。

2. 智能合约开发与部署及测试

智能合约开发是方案设计与实现的关键环节。本研究采用Solidity语言。开发过程遵循严格的安全规范和编程准则，对智能合约进行全面安全审计和漏洞检测，采用形式化验证技术验证逻辑正确性和安全性，确保执行无漏洞错误，同时优化性能，提高执行效率和响应速度。在智能合约开发完成后，部署到区块链网络。采用多节点部署和冗余备份机制，确保高可用性和稳定性。严格控制访问权限，仅授权节点可调用和管理。

3. 分布式存储的数据一致性与测试

分布式存储是该架构的数据存储方式。为确保数据一致性和可用性，本研究采用分布式哈希表（DHT）和纠删码技术。分布式哈希表将数据哈希值映射到网络各节点，实现数据快速定位和存储，使数据均匀分布在区块链网络多节点。纠删码技术将原始数据分割成多个数据块，并生成冗余数据块存储在不同节点。当部分节点故障或数据丢失时，可恢复原始数据，从而保证数据完整性和可用性。采用分布式共识算法Raft算法，通过选举领导者节点协调各节点数据同步和更新，确保所有节点数据一致。在性能测试中，测试不同节点数量下数据存储和读取速度，以及节点故障时数据的恢复能力。

从表2数据可知，随着节点数量的增加，数据存储和读取速度相应提高；当节点故障时，数据恢复成功率也较高。这表明该分布式存储和数据一致性维护方案效果良好。模拟网络测试环境包括多个区块链节点、数据服务器、应用服务器和客户端，部署多种网络攻击场景。安全性测试结果表明，该系统能有效抵御DDoS攻击、SQL注入攻击、数据窃取攻击等。性能测试结果显示，该系统在数据存储、身份认证、智能合约执行等方面性能表现良好，可满足实际应用需求。

结语

本文深入挖掘区块链技术在网络安全领域的应用，打造出综合性解决方案。该方案在防护攻击、守护数据安全和增强网络信任等方面成果突出。当前，区块链在网络安全的应用中还存在性能瓶颈、智能合约安全隐患及与现有技术融合难题等。后续研究将持续完善方案，推动区块链与网络安全深度融合，为网络安全与信息化协同筑牢技术根基。

表1　对比测试数据

加密算法	加密速度/Mbps	密钥长度 / 位	安全性强度（抵御攻能力）
优化前RSA	50	2048	中
优化后ECC	120	256	高
优化前AES	150	128	中
优化后AES	180	128	高

表2　测试结果

节点数量	数据存储速度（MB/s）	数据读取速度（MB/s）	节点故障数据恢复成功率
5	50	45	90%
10	80	70	95%
15	100	90	98%