基于区块链技术的网络信息安全研究

◆金 鑫

摘要：由于互联网和物联网技术的迅猛发展，使得网络空间包含了庞大的数据信息，如何保证这些数据的安全性和隐私性已成为当下工作的重点内容。而以区块链为基础建立起来的用于保护相关数据信息的网络安全机制因其具有不可篡改、可信度高等特点，因此可以作为提升网络空间数据信息的安全性的有力措施。论文主要对基于区块链技术的网络信息安全进行了研究。

关键词：区块链技术；网络信息安全；研究

一、前言

近年来，在互联网和物联网发展背景下，为了更好的满足需求，提高网络服务质量，就需要对相关用户的信息数据进行采集。而采集到的数据过于庞大且较为繁琐，因此通常都是分配给多个不同服务商的数据中心，来对其进行管理与储存。传统的数据存储和管理工作都是由固定的中央机构来完成的，这种情况下，中心节点就成为了极容易受到攻击的部分。基于此，就需要采用区块链技术，来实现对网络信息安全的管理，有效避免传统数据存储和管理中遇到的问题。

二、区块链概述

区块链技术在实际应用过程中采用的是分布式模式，以此确保数据库维护的全面性与整体性[1]。数据块是区块链技术中的重要组成部分，它是将相关数据信息等运用一定的密码学技术进行处理形成的，这些数据块相互独立被称为区块，而将这些独立的数据块根据时间顺序连接起来，则形成了区块链。

在形成的各个区块中，通常包含着一定的时间段，在这个固定的时间段内，都会产生新的信息，例如一些验证标记等。所以一般在进行数据库信息提交和录入的过程中，由于录入到数据库信息不可执行删除和修改等操作，所以在录入时，就必须要经过参与者的确认，从而确保数据库信息的准确性。

三、区块链的核心技术

安全散列算法，通常也被称为“安全哈希算法”。它是针对信息加密等研究出的一种技术。在对相关数据进行运算的过程中，通常都会根据计算出 Hash 值的正反向来确定整个计算难度。如果计算出的 Hash 值为正向，则说明整个计算过程操作简单，反之则证明计算具有较高难度。

区块链网络主要采取的是哈希数计算方式，来构建数据信息的树形结构，其中树形结构中的节点就是上述提到的 Hash 值，以此来检验丰富的信息数据，确保其真实性与完整性。例如，在区块链网络安全零确认中，如果整个交易是以双花子链为渠道开展的，那么想要入侵网络环境的话必须找到强区块，而在此过程前必须要以相应的弱区块为基础。根据显示结果可以得知，在对 500 千字节，并且只提供一分钟的确认时间的区块进行入侵时，通常要使用双花攻击，在此背景下，就需要入侵者掌握一定标准的全网算力，其进行入侵交易所需要支付的费用为 0.2 美元。但是当区块存储容量逐渐上涨时，进行双花入侵交易所需要的费用也将有所提升，其安全系数则会有所降低。在区块链中，每个数据区块都包含着大量的数据信息，而每个区块的加密链接则是由其后边区块来承担，也正是由于这种互相链接的过程，促使了链结构的形成。

四、网络信息安全和隐私保护

基于区块链技术建立的对数据信息进行管理的体系，其核心结构就是它的去中心化，从而有效改变传统中央机构带来的数据风险。正是由于区块链技术的不可篡改、可追溯等特点，因此可以在信息数据管理方面广泛应用，同时确保了数据信息的准确性与真实性[2]。

通常想要保证去中心化系统的正常使用，就需要区块链技术与外部数据库融合，将数据从其所对应的权限中分离出来来完成。相关程序想要获取用户数据信息时，必须以用户许可的前提下来进行。据了解，当应用程序需要进行信息访问时，其请求就会被区块链接收，而想要确认应用程序对信息是否有访问权限，则需要系统对区块链的记录进行检查。如果通过了系统检查，区块链就会对已执行的操作进行记录并将其反馈给应用程序。正是由于区块链具有一定的记录功能，因此使得整个过程操作具有透明化，方便了后期数据的追溯，保证了网络信息安全。另外，还要对网络信息数据的完整性给与重视。KSI 是基于区块链基础上的一种无密钥签名体系。在此体系中，主要是利用单向性的散列函数以及区块链技术的不可篡改性，来达到提升签名可靠性的目的，有效防止了因黑客侵入导致文件被篡改现象的发生，提高了网络相关文件的完整性。

五、物联网权限安全与通信安全

将区块链技术应用到物联网设备中，可以有效避免传统中心化结构带来的网络风险，确保物联网设备以及设备之间通信方面的安全。基于区块链技术形成的对物联网设备进行管理的体系，通常需要一定的权限才可对设备下达任务指令，设备之间的通信情况、权限情况、下达的控制指令等都被记录在了区块链中。具体来讲，在系统运行背景下，物联网设备之间的通信等都必须要以用户授权为前提来进行，在用户授权通过后，系统会分发通信密钥，从而完成设备间的通信与控制，有效保证了物联网设备的安全与隐私。同时，区块链还会对设备间的

（下转第 82 页）

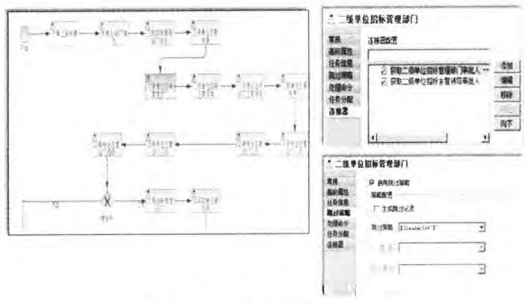

图 5 招标方案审批流程图

4. 招标方案运行状态

提供招标管理人员用户查询浏览各单位、各业务范围的招标方案运行情况，如图 6 所示：

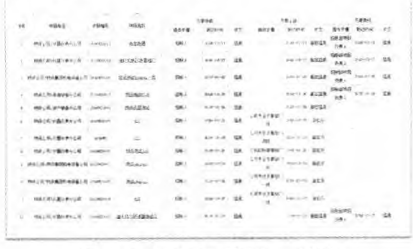

图 6 招标运行情况一览表

四、结语

现系统现已全部上线应用。目前，系统已经运行招标和不招标项目 7567 个，方案总数 9722 个，发布中标结果信息 26 条，中标金额近 1 亿元，系统运行稳定，效果良好，已成功实现电子招投标系统的预期目标，并已达到用户要求。

《大庆油田电子招投标管理系统》招标管理模块的设计与研发，为油田公司招标管理模式带来全新的变化。招标方案数据统一管理，促进信息高度共享，为宏观决策提供参考依据；降低业务成本，规范招标业务，符合无纸化办公理念，提高管理水平。总之，系统功能务实，开发技术先进，伴随着系统功能不断完善与实际应用，具有较大的推广应用前景。

参考文献

[1] 魏鑫 . 石油企业招标综合管理信息系统的设计与实现 [J]. 电子科技大学 ,2012,01.

[2] 董福壮，罗伟其 . XML 在工作流管理系统中的应用 [J]. 计算机工程与应用 , 2012,33.

（作者单位：大庆油田有限责任公司勘探开发研究院）

（上接第 79 页）

通信或控制全过程按照时间顺序进行详细记录，并且将专门负责记录指令的区块给与明确，只有在区块对设备身份和权限进行确认后，所下达的指令任务才能完成执行，这样不仅保障了物联网设备的安全性，而且其信息数据的机密性与完整性也得到了有效提升。

六、抵御 DDoS 攻击

DDoS 攻击者会利用大量技术手段，来向所攻击目标的节点发出请求，从而占据系统中心节点的网络空间与资源，使攻击目标系统处于网络瘫痪状态。传统网络系统主要依靠各节点来提供相应服务的，通常来讲，无法抵御此类攻击。而基于区块链技术的系统，可以将数据信息分布于多个网络设备中进行存储，具有去中心化特点，因此也就不存在系统中心节点，DDoS 也就无法对系统进行攻击。同时，区块链各个节点都包含着丰富的数据信息，虽然其作为独立个体存在于区块链当中，但是每个节点都可以对区块链中的其他节点产生作用，并且各节点都可以对其他网络节点信息的有效性进行检验。所以即使区块链中的某个节点被攻击，也不会发生系统瘫痪等情况，仍然可以利用各节点的独立性，使得未被攻击的节点继续在区块链中发挥作用，保证了整个区块链系统的正常运行，从而对已经被破坏的节点数据进行修复。由此可见，利用区块链技术可以建立一个抵御 DDoS 的攻击的数据库系统。

而在域名系统（Domain Name System 缩写 DNS,Domain Name 被译为域名）中应用区块链技术，可以有效防止因 DDoS 造成单点失败等现象，从而保证整个网络系统的安全。目前基于区块链而建立的域名系统最具代表性的就是 Blockstack。它主要由三部分结构构成，即区块链、数据库以及云存储。而 Blockstack 系统则是由多个逻辑层构成的，区块链技术一般处于整个系统的最底层，来对整个系统执行的具体操作以及文件散列值等进行记录，它也是保障整个系统安全与可靠的关键所在。路由层主要是为系统提供自身区域内的文件散列值传达到区域文件路径的映射。这样用户在接受到系统地层传输的散列值后，路由器就可以根据散列值来对相关文件进行精确查找。而系统存储层主要是对系统信息数据进行存放的区域，在经过上述流程获得相关区域文件后，就会使数据信息的存储路径得以明确，存储层内就会将目标数据传达给用户。

七、结语

综上所述，随着时代的不断发展与进步，传统的网络信息保护机制已然不能保护网络信息的安全，基于此，就需要相关业内人士对此问题给与重视，及时运用区块链技术，从而使用户信息、重要数据以及基础设施等都能受到全面有效的保护，更好的营造一个安全的网络环境。

参考文献

[1] 房卫东，张武雄，潘涛，陈伟，杨旸 . 区块链的网络安全：威胁与对策 [J]. 信息安全学报 ,2018,3(02):87-104.

[2] 陈烨，许冬瑾，肖亮 . 基于区块链的网络安全技术综述 [J]. 电信科学 ,2018,34(03):10-16.

（作者单位：江苏省宿迁经贸高等职业技术学校）