基于区块链技术的数据存储和传递系统设计

徐新梅
杭州宇链科技有限公司　浙江　杭州　310000

摘　要：针对网络安全系统中一些关键数据存储的安全性，设计了基于区块链技术的数据安全存储处理系统。首先，本文分析了其控制系统和网络安全系统的架构；然后，基于区块链的技术原理，设计了具体的安全数据存储处理系统，给出了应用部署的架构，分析了数据安全存储处理过程；最后，对所设计的系统进行了实际的测试验证。

关键词：数据安全；区块链；工控安全；密码算法；网络安全

引言

在信息化时代，信息成为了各行各业必不可少的重要战略资源，应用云计算技术能够形成全新的数据储存及处理方式。但是，由于云计算开放性的特点，在数据储存及共享过程存在一定的安全威胁，数据储存中心在经受攻击毁坏之后，将会使关联的服务器系统出现严重故障，导致数据泄露。

1 区块链技术原理

区块链技术凭借分布式去中心化、信息安全性、智能化等优势，将其与商业银行相结合必将改变其传统商业模式，触发新一轮金融领域变革的浪潮，助推经济结构转型升级，实现跨越式高质量发展，为此，需要对区块链技术的概念、特点以及分类有清晰的了解，厘清区块链技术与经济社会要素优化配置之间的辩证关系。区块链是将按时间先后顺序的块连接在一起而形成的一种数据结构，块是最微小的承载，块与块之间联合发挥作用来表示数据信息。在每块中设有时间戳标记，以实现区块链的可追溯性与安全性。随着信息技术的不断发展，区块链作为一种新型技术逐渐被人们接受并应用于各个领域。由于区块链的非中心化、分布式记账、不可篡改等特性，将会是未来金融业的发展方向。以区块链技术为支撑，能够很方便地实现信息采集、加工、记录与存储等流程。借助区块链技术，银行和其他金融机构只要通过节点查询和核验企业信息，就可以达到数据授信的目的，并且在交易过程当中，可以通过区块链时刻监管交易进程，保证交易安全。

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，被誉为Web3.0时代最关键的底层代码。为应对纷繁复杂的业务场景需求，我国区块链技术正朝着以下4个方向发展：一是数据传输更加精准迅速，达成更大范围的数据协同，逐渐成为当前阶段区块链技术发展的主题；二是网络规模更加广泛，越来越多的企业开始将目光聚焦于跨链技术的研发与创新，实现衔接区块链之间的信息孤岛；三是技术运维更加精细，正在逐步完善账户角色体系、账本数据量控制体系、特殊场景应对技术、平台运维技术等技术体系；四是平台安全更加可控，链上同态加密、国密算法、群环签名等创新安全技术相继出现，区块链平台安全应用技术加快落地。

2 系统功能设计

系统的结构分为链上和链下两部分。链下部分是由Mysql与Redis数据库组成的，Mysql主要负责存储本地数据，Redis存储数据索引和加密数据。链上部分分为搭建区块链网络，编写链码，使用SDK，搭建基于浏览器的用户接口。系统的结构及功能如图1所示。链上+链下的设计思路是将本地数据保存在Mysql数据库中，通过加密算法生成密文和数据的hash值，将密文和hash值存储到区块链上的同时，也将hash值在本地Redis数据库中保存一份，由于需要在本地存储的是 < hash值：加密值>的数据格式，符合Redis的K-V存储架构，所以采用Redis存储。在查询的时候，可同时查询链上的hash值和链下的hash值，如果两个hash值相同说明数据正确，随即解密数据。使用Go语言编写链码，并在链码中定义对数据操作的函数。与之对应的也要在调用SDK时采用相同的函数名。前端展示采用SpringBoot和Jquery，Bootstrap等框架。系统功能方面主要有登录、本地查询、数据上链、链上查询、数据解密这些功能。其中，本地查询和登录时在本地的数据库上进行操作，并不涉及区块链网络。而数据上链、数据解密、链上查询这些操作则是运行在区块链网络之上。系统分为链上和链下两部分的好处：一是可以缓解区块链上由于数据增大带来的性能问题，二是可以做到链上链下数据结合，进一步确保数据的安全性。

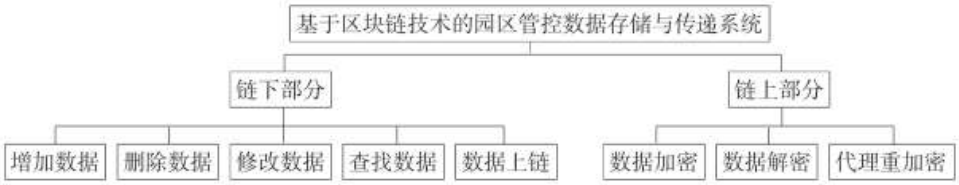

图1 系统结构

3 区块链技术的数据存储和传递系统设计

3.1 区块链底层设计

HyperledgerFabric区块链网络在当前的系统方案设计中，主要是储存框架的主干区域结构。作用于区块链联盟，HyperledgerFabric区块链网络的应用本身涵盖了众多基于联盟链中的特征表现，能够实现更加完善的开源作用效果。在HyperledgerFabric区块链网络结构中，以网络组织作为单位进行计算，便于实施联盟式组织管理工作、初始化系统，将每一组织中的证书向其他的组织进行传递共享，或是由对应的组织自动生成证书，后续由所属组织对证书进行维护。HyperledgerFabric联盟链的架构涵盖了身份管理、账本、交易以及智能合约部分。身份管理结构则是对不同的网络进行判断，是否能够给予其进入到联盟链的许可。一般情况下，HyperledgerFabric考虑到区块链数据云储存及共享过程中大多数处于商业应用状态，因此，对于审计、隐私、安全和性能等的要求相对较高，需要构建较高的准入门槛，保障在内部的各组织成员本身均通过MSP服务认证，才能够准许进入到网络中。而PKI的公共钥匙基础设施结合去中心化的区块链机制，促使HyperledgerFabric的功能更加强大，能够为整体联盟链状态下的网络内部组织成员提供审计、隐私保护以及身份验证等众多功能。

3.2 数据安全存储处理过程

网络安全系统的关键数据存储处理的核心在于利用区块链技术进行数据存储。区块链系统本质上是一种分布式存储系统，最大的特点是区块链上存储的数据具有不可篡改的特性。区块链由大量区块首位相连链接而成，第一个区块为创世区块，区块数量随着数据的不断存入而不断增长，数据的存入由区块链系统中的矿工成功挖矿而确定下来。

区块链系统中的某一区块的结构如图2所示。在区块中的Tx1、Tx2、Tx3、Tx4即是用来存储数据的。基于区块链的数据存储处理过程如下：首先，在网络安全系统中，态势感知平台或数据探针提取得到重要的日志、事件等关键数据；然后分别打包发送到数据存储服务器，数据服务器通过SHA256算法提取数据包的摘要P1、P2、P3等存入区块链系统中当前区块的交易信息Tx1、Tx2、Tx3中；最后，当当前区块的Tx1到Tx4都存储完毕时，区块链系统发起挖矿通知，由挖矿成功的节点将当前区块正式存入区块链并进行广播，由所有节点进行接收和验证。

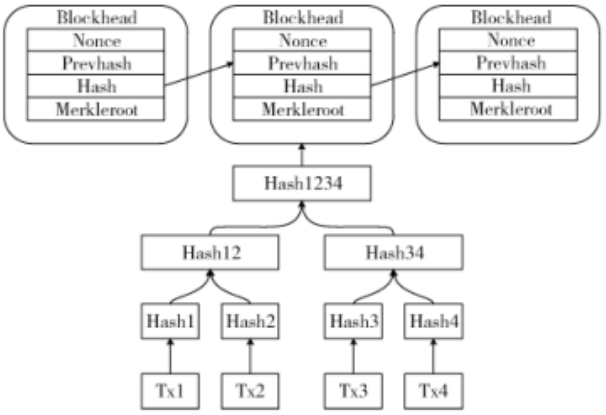

图2 区块链中的区块结构

3.3 链上+链下存储

将数据存储在区块链上虽然能保证存储的数据不被修改，但是无法保证存储的数据是否正确。而且在区块链上存储过多的数据也会导致区块链的性能下降，针对这种问题采取链上+链下的设计模式。链上与链下分别存储路径的不同计算值，这样即避免了数据明文直接暴露，也可以结合链上链下数据两者进一步确认数据的正确性。数据经过哈希运算后得到的是固定长度的一串字符串，所以在链上存储数据的哈希值可以减轻区块链的存储查询压力，同时存储在区块链上的数据还包括本地的存储路径以及密钥。在本地存储数据的加密值以及数据的哈希值。在数据上链的时候，将数据进行加密和哈希运算，数据的加密值存储在本地，数据的哈希值同时存储在本地和区块链网络上。在解密的时候，同时对比链上和链下的数据哈希值是否一致。如果一致，则说明数据没有被修改，然后查询在区块链网络上的密钥以及本地数据存储路径，将数据解密。

4 建议

4.1 提高财务数据信息存储的安全性

财务数据信息安全是区块链应用于企业财务管理的

根本。在传统的企业财务管理模式下，受到组织架构、利益冲突、数据管理方法等因素影响，企业财务管理过程存在不同程度的信息失实情况，数据造假现象层出不穷。在区块链技术干预的企业财务数据信息采集、流转、分析场景下，只要某部门或子公司提交一笔交易申请，交易账目信息就会形成全网无重复记录数据库，依据各自产生时间顺序形成闭环链条，并被记录在单独的唯一的区块中，随后上传至全网，由上下游的其他区块检索比对，校验其真实性。在确认其真实有效之后，将哈希值与前一个区块互联互通，识别前一区块哈希值以及时间戳，将信息保留并传递至后一区块，随后完成数据的留存。需要说明的是，因为区块链技术自身的“阻拦性”，目标区块的数据信息只有经过共识机制标注认可之后才能生成有效信息，加之哈希算法加密是不可逆的，因此，区块链下生成的会计核算信息将会是一个不可篡改的财务账本，无法擦除和篡改。显然，在数据管理方面，与现行的会计核算信息一般管理相比，区块链技术中的多方共识机制、基于密码学的加密算法（哈希算法），使得企业财务数据信息写入需要全网节点共识认证，且一旦被写入就会被加盖时间戳，按证书、时、空维度精准记录。如果要修改区块链中的财务信息，必须征得超过整体一半比例节点的同意，并对区块链上所有节点信息进行修改。基于此，区块链可提高财务信息溯源能力，令链条上数据信息无法被仿冒和销毁，并将合约信息传播到每一节点，以链的方式前后存储，继而减少在确认、记录、计量和报告环节被修改、删除、伪造的可能性，满足财务数据安全要求。

4.2 区块链技术在企业财务数据存储中的具体运用

在当前在线存储大为流行的数字存储时代，区块链上的整个数据链都是加密状态，能够建立具有结构化的数据系统，提升财务数据信息的可靠性和准确性。其中，在企业财务管理过程中，区块链技术下的分布式存储，因其不可伪造、难以修改、全留痕、可追溯性等特点，备受企业财务数据存储追捧。就内涵而言，分布式存储是一种将数据存到多台机器上的存储技术，其区别于传统的集中存储结构，并不是把数据集中放于同一个设备或者系统之中，而是采用可扩展的系统结构，把存储资源打碎打散，并将其存储于后端大规模分布式存储系统。在区块链技术的应用过程中，分布式存储执行了去中心化运行机制，使得分类账不再依靠特定个人、特定机构，可以分布在多个节点上，区块链可以同步记录并稽核全部节点中的事务，并支持用户链上数据共享，推动企业财务数据资源得以跨平台、跨协作、跨格式存储和分享。就实践而言，作为一个分散的数据库技术，企业财务管理中的区块链存储技术，允许记录产品来源以及其他数据，经常使用分布式协同技术来管理财务管理数据资源，防止财务数据丢失和失真，避免审计中的舞弊行为。

结语

本文设计的系统解决了在没有中心服务器的情况下公司之间安全可信的传递数据的问题。系统分为链上和链下两部分。链下部分是对本地数据库的增删改查以及加密上链操作，通过增删改查操作获取需要的数据，点击数据上链即可加密数据并将数据的哈希值存储到区块链，将数据的加密值和数据存储路径以及代理重加密密钥存储到本地数据库。在完成基础功能的同时实现了代理重加密，链上+链下存储等，优化了系统的操作和使用，为类似的系统提供了一定的参考价值。

参考文献

[1]贾朋飞.基于区块链的笔录系统的研究与实现[D].北京：中国人民公安大学，2021.

[2]张召，田继鑫，金澈清.链上存证、链下传输的可信数据共享平台[J].大数据，2020,6(5):106-117.

[3]刘尚，郭银章.云计算多授权中心CP-ABE代理重加密方案[J].网络与信息安全学报，2022,8(3):176-188.