区块链技术在电子政务数据共享中的安全机制设计与实践

刘启贤

深圳华云信息系统科技股份有限公司佛山分公司，广东省佛山市，528000；

摘要：随着数字政府建设的深入推进，电子政务数据共享已成为国家政务服务能力建设的重要内容。如何保障数据共享过程中的安全已成为关键问题，区块链技术在数据共享领域具有天然的优势，本文提出一种基于区块链技术的电子政务数据共享安全机制，详细介绍了总体架构设计、数据加密与隐私保护措施、智能合约在安全机制中的应用，以及在典型场景下的应用实践。通过使用区块链技术，可以实现电子政务数据在不同主体之间共享时的身份认证和访问控制，确保数据安全，提高效率。基于此安全机制设计，本文设计了一套电子政务数据共享系统并进行了部署实践。

关键词：区块链技术；电子政务；数据共享；安全机制设计

DOI：10.64216/3080-1508.25.09.064

引言

当前，随着政府数字化转型进程的加速，电子政务数据共享已成为数字政府建设的重要内容，而数据共享过程中存在的安全问题也日益突出，主要表现在数据隐私保护、访问控制和数据完整性等方面。针对传统电子政务数据共享存在的安全隐患，本文提出了一种基于区块链技术的电子政务数据共享安全机制设计方案，该方案基于区块链技术可以实现在不同主体之间数据共享时的身份认证和访问控制，以保证电子政务数据在共享过程中的安全性和保密性，同时实现数据在不同主体之间的完整性校验与校验结果验证。本文详细介绍了安全机制的设计与实现过程。

1 区块链在数据共享领域的优势分析

区块链技术（Blockchain）是一种去中心化的分布式账本数据库，它由分布式节点组成，是一种加密货币和智能合约等应用的底层基础设施，具有去中心化、不可篡改、可追溯等特点。在数据共享领域，区块链技术的优势主要体现在以下几个方面：去中心化：区块链技术不依赖于特定的组织机构，不受时间和空间限制，通过去中心化的方式进行数据传输和存储。可追溯：区块链上的每一个数据记录都可以在其他节点进行溯源查询，确保数据真实性与可靠性[1]。安全性高：区块链采用智能合约进行交易，极大提高了数据交换与共享的安全性。

2 区块链技术在电子政务中的应用现状

当前，电子政务数据共享的应用已取得了一些成果，例如电子政务平台的数据共享功能在政务服务中已得到广泛应用。但电子政务数据共享过程中仍存在诸多安全隐患，如身份认证和访问控制机制不完善、数据共享过程中的隐私保护、数据的完整性校验等。此外，由于区块链技术本身存在的缺点，如安全性和可靠性问题、计算能力有限、缺乏法律保护等，使得区块链技术在电子政务数据共享中的应用仍有一定的局限性。因此，亟须研究一种基于区块链技术的安全机制来解决这些问题，以提高电子政务数据共享的安全性和可靠性，保障电子政务数据共享过程中各主体间的信息安全。

3 电子政务数据共享的安全需求分析

3.1 电子政务数据共享的现状与挑战

在传统电子政务中，由于各部门之间信息壁垒的存在，使得各部门之间难以实现数据共享，在这种情况下，政府需要建立一个数据共享平台来解决各部门之间的数据共享问题。然而，由于传统电子政务平台建设时间较早，其存在的弊端也日益突出，主要表现为：（1）各部门之间信息壁垒：（2）平台建设不统一：（3）缺乏安全保障：（4）数据共享机制不完善：由于上述问题的存在，导致电子政务数据在不同部门之间进行共享时，往往需要进行多次的身份认证和访问控制，并且还需要对数据进行完整性校验和结果验证。这些安全隐患使得电子政务数据共享过程变得复杂且效率低下。

3.2 数据安全需求（隐私保护、访问控制、数据完整性等）

在电子政务数据共享中，由于各部门之间存在着利益冲突，使得数据共享过程中的信息安全和保密问题尤为突出，因此，对数据共享过程中的隐私保护、访问控制和数据完整性等方面的要求也就尤为突出。数据隐私保护是指在电子政务数据共享中，对涉及个人隐私或敏感信息的数据进行加密或脱敏处理，从而防止其他组织或个人非法获取；访问控制是指在电子政务数据共享过程中，根据不同主体的业务需求，对数据访问权限进行

控制，防止其他组织或个人非法访问；数据完整性是指对电子政务数据在传输和存储过程中的完整性进行校验和验证[2]。

3.3 传统安全机制的不足与改进方向

在传统电子政务数据共享过程中，由于各部门之间信息壁垒的存在，使得电子政务数据共享过程中存在着大量的安全隐患，具体表现为：（1）电子政务数据共享平台缺乏安全保障：（2）电子政务数据共享平台缺乏身份认证和访问控制机制：（3）电子政务数据共享平台缺乏数据完整性校验机制：（4）电子政务数据共享平台缺乏行为审计机制。针对以上问题，本文提出了基于区块链技术的电子政务数据共享安全机制，通过引入区块链技术来解决传统电子政务数据共享中存在的安全隐患，从而实现电子政务数据在不同部门之间进行有效的交换和共享。

4 区块链驱动的电子政务数据共享安全机制设计

4.1 系统总体架构设计

在基于区块链技术的电子政务数据共享安全机制中，数据共享平台、用户和角色之间通过加密的方式进行通信，利用区块链中的共识机制来确定不同主体间的安全权限，从而保证数据在各主体之间的传输和存储过程中不被篡改。同时，采用智能合约技术来保证数据在共享过程中的完整性。此外，由于电子政务数据共享涉及多个部门，为了保证电子政务数据共享平台能够实时监控和检测电子政务数据共享过程中的异常行为，需要引入异常监测和应急响应机制[3]。基于上述设计思路，本文提出了一套基于区块链技术的电子政务数据共享安全机制方案。

4.2 身份认证与授权机制

身份认证与授权机制是数据共享安全机制中的核心模块，通过该模块，实现对各主体在数据共享过程中的身份认证与授权，确保电子政务数据在各主体之间传输和存储时的安全与可靠。具体来说，身份认证与授权机制主要由两部分组成：（1）基于私钥签名的身份认证：（2）基于公钥加密的身份认证：具体来说，身份认证在该模块中采用了 PKI 技术来实现，用户和角色之间通过数字签名技术来建立私钥，而公钥则由公钥证书和用户公钥共同构成；在用户与角色之间则采用数字签名来进行身份认证，从而保证用户的唯一性；在角色与角色之间则采用数字签名来进行身份认证。

4.3 数据加密与隐私保护措施

在电子政务数据共享安全机制中，数据加密与隐私保护措施主要是指对涉及个人隐私或敏感信息的数据进行加密，从而实现数据在不同主体之间的传输和存储。在该模块中，数据加密与隐私保护措施主要包括以下几个方面：（1）使用散列函数进行加密：（2）使用对称加密技术对数据进行加密：（3）使用非对称加密技术对数据进行加密：（4）使用零知识证明技术对数据进行加密。此外，由于区块链网络节点是由多个节点构成的，因此，在数据共享安全机制中，还采用了共识机制来保证数据在不同主体之间的传输和存储过程中不被篡改[4]。

4.4 数据访问与操作日志记录

在基于区块链的电子政务数据共享安全机制中，对于访问和操作日志的记录主要包括以下几个方面：（1）用户在访问和操作电子政务数据共享平台时，需要首先对电子政务数据共享平台进行身份认证，然后才能够进入到电子政务数据共享平台中；（2）用户在访问和操作电子政务数据共享平台时，需要首先向电子政务数据共享平台提交一系列的凭证信息，例如用户的账号信息、访问权限凭证、身份凭证等；（3）用户在访问和操作电子政务数据共享平台时，需要向电子政务数据共享平台提交相应的访问与操作日志，从而实现对不同主体之间的访问与操作进行记录。

4.5 智能合约在安全机制中的应用

智能合约是一种以计算机代码的形式实现的合同，能够实现合同双方之间的权利和义务关系。在基于区块链的电子政务数据共享安全机制中，智能合约主要应用在以下几个方面：（1）身份认证与授权机制：（2）数据共享与传输安全机制：（3）数据加密与隐私保护机制：（4）数据访问与操作日志记录机制；（5）智能合约在电子政务数据共享安全机制中的应用还包括以下几个方面：（1）对访问权限进行控制：（2）对数据传输和存储过程中的完整性进行校验：（3）对电子政务数据共享平台的行为进行审计与监控；（4）对电子政务数据共享平台进行审计与监控。

4.6 异常检测与应急响应机制

异常检测与应急响应机制是为了解决电子政务数据共享过程中出现的异常行为，从而确保电子政务数据共享安全。在异常检测与应急响应机制中，通过对数据共享过程中出现的异常行为进行分析，从而找到触发该异常行为的具体原因。同时，电子政务数据共享平台需要建立应急响应机制来应对各种可能出现的突发事件，保证电子政务数据共享过程中出现的异常情况能够被

及时发现和处理。

5 区块链安全机制在电子政务数据共享中的实践

5.1 典型应用场景介绍

本文提出的安全机制，通过区块链技术实现不同主体之间的身份认证和访问控制，满足了数据在不同主体之间共享时的安全性与保密性要求，具体应用场景如下：（1）基于数字证书的身份认证与访问控制：通过数字证书实现电子政务数据在不同主体之间共享时的身份认证和访问控制，可解决传统电子政务数据共享中存在的隐私保护、访问控制和数据完整性等问题。（2）基于智能合约的数据交换与共享：通过智能合约实现数据交换与共享，可解决传统电子政务数据交换与共享过程中存在的安全隐患，提高电子政务数据交换与共享效率[5]。

5.2 系统开发与部署实践

通过对数字证书、智能合约的研发，本安全机制可实现基于数字证书的身份认证和访问控制，并可根据实际需要灵活配置不同的应用场景。该系统通过区块链技术实现电子政务数据交换与共享的全过程管理，可广泛应用于智慧城市、社会保障、社会治理等领域，提供数据共享、数据安全、数据管理等功能。以“大联动·微服务”平台为例，本系统部署在政务云平台上，实现了多部门之间的数据共享和交换，具有良好的安全性与稳定性。同时，该系统还支持与其他系统和平台的对接，可在政务云平台上完成跨部门的业务协同、业务办理和业务查询等工作。

5.3 安全机制实施过程

基于电子政务数据共享系统的安全需求，设计了“大联动·微服务”平台的数据共享安全机制，具体实现过程如下：（1）对于用户，根据自身业务需求，对相关数据进行授权和解密，获得对应的访问权限；（2）对于系统，则对授权的用户进行身份认证，并根据角色进行访问权限分配；（3）对于数据共享，则使用智能合约对相关数据进行加密，并通过区块链技术实现数据安全共享；（4）对于业务办理，则使用电子证照等数据进行授权和解密；（5）对于业务查询和统计，则使用电子证照等数据进行授权和解密。

5.4 实践效果与性能评估

平台实践运行以来，得到了良好的效果，具体包括：（1）对于用户来说，能够安全地实现电子证照等数据的授权和解密，并以加密数据的方式进行安全共享；（2）对于系统来说，能够在实现用户身份认证和访问权限分配的同时，也保证了数据共享的安全性；（3）对于平台来说，能够根据业务需求，对部分数据进行加密处理，并以区块链方式进行安全共享；（4）在运行期间，由于采用了区块链技术的去中心化特点，因而不存在任何单点故障问题；（5）对于系统而言，能够在一定程度上保障业务办理过程中信息传输的安全。

5.5 用户体验与反馈分析

用户在使用平台过程中，一方面，能够通过身份认证功能完成用户身份认证，并以加密数据的方式进行安全共享；另一方面，能够通过智能合约功能，将用户对电子证照等数据的授权和解密操作进行自动执行，以保证平台运行期间数据的安全性。从用户体验来看，由于区块链技术本身的去中心化特点，因而不存在任何单点故障问题，因而能够保障用户在进行数据共享时的安全性；同时，由于智能合约具有自动执行的特点，因而不存在任何人工干预操作的过程，从而能够保证平台运行期间数据的安全性。此外，平台还可以通过区块链技术实现数据共享、查询、查看等功能。

6 结语

区块链技术是当前数据安全领域中的一项新兴技术，其在数据共享过程中具有去中心化、防篡改和可追溯的特点，因而能够有效保障数据共享的安全性。本文以“电子证照”为应用场景，设计了基于区块链技术的安全机制，并在该机制下进行了实践验证。实验结果表明，该安全机制在实现数据共享功能的同时，能够保证数据共享过程中的安全性，为区块链技术在电子政务中的应用提供了一种新思路。随着区块链技术的不断发展与成熟，其在电子政务领域中的应用也将越来越广泛，为提高政府治理能力、提升政府服务效率和改善人民生活水平提供了新的技术手段。

参考文献

[1]马晓峰.基于区块链技术的电子政务信息数据加密与共享方法[J].电子元器件与信息技术,2025,9(03):9-11.

[2]周海涛.基于区块链的可信政务系统数据绩效评价分析[J].电子技术,2025,54(03):118-121.

[3]翟文佼.区块链背景下电子政务现代化创新管理研究[J].生产力研究,2025,(03):36-42.

[4]张叶.区块链驱动的公共卫生风险跨部门协同治理研究[D].中南大学,2024.

[5]刘星宇.区块链技术应用于干部个人信息管理的研究[D].云南财经大学,2024.