区块链赋能社保卡一卡通数据安全与隐私保护

史阳

辽宁省社会保险事业服务中心，辽宁省沈阳市，110000；

摘要：本文主要研究区块链对社保卡一卡通数据安全与隐私保护，描述了社保卡一卡通的发展情况以及遇到的数据安全和隐私问题，分析区块链技术的特点对保障数据安全和隐私的优势，探讨区块链在社保卡一卡通方面的数据存储、传输、访问控制等的应用研究，研究智能合约实现数据管理和隐私保护规则自动执行的方法，研究结果表明，区块链可以有效提高社保卡一卡通数据的安全性、私密性，为社保卡一卡通系统的稳定运行提供有力的支持，推动社会保障事业高效发展。

关键词：区块链；社保卡一卡通；数据安全；隐私保护

DOI：10.69979/3041-0673.26.04.103

社保卡是民生服务的基础性载体，在信息技术飞速发展的情况下，社保卡一卡通作为社会保障领域的重大革新，将人社服务、就医购药等基本功能整合起来，并且慢慢延伸到金融支付、公共交通等方面，成为便捷服务的载体。但是它在实现多功能的集成以及广泛覆盖的同时，也面临着严峻的数据安全和隐私保护问题。系统中存在大量的个人敏感信息，如果受到攻击或者泄露，会直接侵害到用户的权益，并且还会对社会保障体系的稳定运行造成影响。区块链技术依靠去中心化、不可篡改、可追溯这些技术特性，给上述问题的解决赋予了新思路。利用区块链技术来应用社保卡一卡通系统，可以有效的提高数据的安全性以及隐私性，切实的保障民众的信息安全以及合法权益。

1 社保卡一卡通发展现状与挑战

1.1 发展现状

社保卡一卡通已经由单一的社会保障功能，逐步发展为集社会保险、医疗健康、金融支付、公共交通、文化旅游、待遇发放等多功能为一体的综合性服务平台。持卡人可以凭借此卡享受就医购药费用结算等便捷的医疗服务，也可以在银行网点或者合作商户存取款、消费等。目前社保卡一卡通已在全国范围内大量发行，覆盖各个年龄段的人群，可以在线查询社保信息，办理相关业务等，极大地方便了人民群众的公共服务，是我国社会保障服务体系的重要载体。

1.2 社保卡系统面临的主要安全风险

1.2.1 数据泄露风险

社保卡是集身份证、社保信息、医疗记录、金融账户等多种个人敏感信息于一身的多功能集成载体。此类信息如果泄露，就会被用于诈骗、盗刷等违法活动，对持卡人权益造成潜在的威胁。目前系统所面对的外部网络攻击以及内部操作风险，均有可能成为数据泄露的诱因，需要采用技术和管理手段加以防范。

1.2.2 数据篡改风险

社保卡系统是个人社会保障权益的电子化载体，其存储数据的真实性、完整性是系统可靠运行的基础。业务流转当中，若对缴费记录、个人账户信息这些重要数据予以篡改，就会出现待遇计算及发放失误的情形。此类风险来自于系统漏洞、权限管理缺陷或者传输环节的安全隐患，可能造成个人权益受损、资源分配不公，甚至影响社会保障制度的公信力与可持续运行。所以建立防止篡改的数据保障机制对社保卡系统安全来说非常重要。

1.2.3 隐私侵犯问题

多部门数据共享机制容易造成隐私泄露，缺少严格约束的时候，协同机构会获得超出范围的用户敏感信息，有些主体还会对数据进行过度收集、分析，然后将其用作商业用途，从而增大个人隐私被侵犯的风险。

2 区块链技术特性及其在数据安全与隐私保护方面的优势

2.1 区块链技术特性

2.1.1 去中心化

区块链技术采用分布式的架构，不是依靠某个中心节点，每一个参与方都有一个完整的主体副本，通过共

识机制来保证数据的一致性。该架构可以降低中心节点故障或者遭受攻击时所造成的系统性风险。同时区块链中的交易记录具有公开可验证的特点，可以提高系统的透明度与可信度。

2.1.2 不可篡改

区块链使用哈希链式结构来保证数据的不可篡改性。每个新区块包含上一个区块的哈希值，构成前后相连的一条链。任何对历史数据的修改都会导致该区块哈希值发生改变，进而引起后续所有的区块哈希值发生连锁反应。网络节点利用共识算法来验证区块是否有效，如果发现哈希值不对就会拒绝这个错误的数据。这种链式验证机制从技术上保证了数据的真实性、完整性，使得篡改行为在分布式网络环境下几乎不可能完成。

2.1.3 可追溯性

区块链会把每笔交易的时间戳以及流转路径都完整地保存下来，这样就可以对数据的整个流程实施溯源，在社保的应用当中，可以针对医疗费用等关键的操作来源去向展开细致的追踪，有效地杜绝欺诈行为的发生，而且给监管赋予透明又可信的审计凭证。

2.1.4 智能合约

智能合约就是部署在区块链上的一种自动化的协议，当满足事先设定的条件时就会自动执行相应的操作。不可更改的代码被用作社保卡系统权限控制和数据管理工具，并且可以实现访问权的自动检测以保证隐私规则得到高效的、可靠的实施效果。

2.2 在数据安全与隐私保护方面的优势

2.2.1 增强数据安全性

区块链由于去中心化存储、不可篡改的特性，能够有效降低数据泄露和篡改的风险。社保卡系统当中，敏感信息分布式存储可以消除中心化数据库单点被攻破的风险。加密技术结合，保证数据只有授权人才能解密访问，从存储和传输两个方面加强安全性能[1]。

2.2.2 保护个人隐私

区块链+隐私计算=数据可用不可见。用户可以不用透露自己的医疗信息就可以完成业务的验证，防止用户的隐私被泄露，所有的数据使用记录都可以被追踪到，所有的数据都是在符合隐私规范的情况下使用的，不会出现信息被滥用的情况。

2.2.3 提高系统可信度

区块链透明、可追溯，所有交易记录都是公开的，用户和监管者共同监督系统运行，共识机制使得数据在全网范围内一致，避免了由于信息不透明或者版本不同而产生的争执，从而提高了系统公信力，使社保卡的应用得到推广并赢得信任。

3 区块链在社保卡一卡通数据安全与隐私保护中的应用

3.1 数据存储环节

3.1.1 分布式存储

区块链把数据分散到很多节点上，用分布式存储，社保卡一卡通系统可以将个人敏感信息分成几部分，分别存到不同的节点上。如果某个节点被攻击或者发生故障，也不会导致整个数据的安全性和完整性出现问题，而且可以提高数据的可用性和可靠性，从而保证用户随时可以访问自己的数据。

3.1.2 加密存储

为了保证数据的安全，区块链把保存在节点里的数据加密处理。采用对称加密或者非对称加密算法对个人的敏感信息进行加密，只有拥有对应密钥的人才能解密并访问这些数据，在社保卡一卡通系统中给每个用户生成一个唯一的密钥对，使用公钥加密数据，私钥解密数据，即使有人截获了数据在传输或者存储过程也无法对其进行解密，从而保证了数据的安全性。

3.2 数据传输环节

3.2.1 安全传输协议

区块链使用 SSL/TLS 协议保证数据在传输过程中的安全性。社保卡一卡通系统用户上网访问时采用 SSL/TLS 加密传输协议，防止数据传输过程中被窃取或篡改。区块链可以采用数字签名技术，对传输的数据进行签名，保证数据的完整性、真实性[2]。

3.2.2 点对点传输

区块链的点对点传输特点，数据在传递过程中不会经过中心节点，降低了被截获或者攻击的风险。社保卡一卡通系统用户可以与其它节点直接通信，并且可以实现点对点数据交换。

3.3 数据访问控制环节

3.3.1 基于属性的访问控制

区块链可以采用基于属性的访问控制机制，用用户身份、角色、权限等信息来对数据进行访问。在社保卡

一卡通系统中，给不同的用户赋予不同的属性，普通用户只能看到自己的基本信息和社保记录，医疗机构可以查看用户的医疗记录，基于属性的访问控制可以实现对数据的精细化管理，使授权人员可以访问到相应的数据。

3.3.2 智能合约实现访问控制

智能合约可以实现数据访问控制的自动执行。在社保卡一卡通系统中可以编写智能合约来规定数据的访问规则。像当用户想要访问某一块数据的时候，智能合约就会自动识别用户的身份以及权限，只有符合条件的用户才会被允许访问。智能合约的执行是自动的、不可篡改的，可以避免人为因素造成的访问控制失误，提高了数据访问的安全性、可靠性[3]。

3.4 隐私保护环节

3.4.1 零知识证明

零知识证明属于隐私保护技术，可以不对具体信息进行泄露，只是去证明某一个陈述是正确的。在社保卡一卡通系统中可以应用零知识证明技术来保护个人隐私，用户想要证明自己年龄满足某项业务要求的时候，就可以利用零知识证明技术，不透露确切年龄的情况下向系统证明自己符合要求。

3.4.2 同态加密

同态加密就是对加密数据进行运算处理的一种加密技术，对于社保卡一卡通系统来说，可以利用同态加密技术对个人的敏感信息实施加密，然后再对这些加密数据执行计算和分析操作。医疗数据分析时，可以对加密的医疗记录执行统计分析等操作，而无需解密数据，在整个过程中既能对数据展开分析利用，又能保障个人信息的隐私。

4 区块链赋能社保卡一卡通数据安全与隐私保护的实施策略

4.1 技术层面

4.1.1 选择合适的区块链平台

目前市场上有很多种类的区块链平台，以太坊、超级账本等，在进行区块链赋能社保卡一卡通的数据安全与隐私保护研究时，要根据系统具体的需求和特点选择合适的区块链平台，如果系统对性能要求较高，则可以选择吞吐量大、延迟低的区块链平台；如果系统重视隐私保护工作，则应选择具有较为先进的隐私保护技术的区块链平台。

4.1.2 优化区块链性能

区块链技术目前还存在着交易处理速度慢、吞吐量小的缺陷，想要使区块链在社保卡一卡通系统中使用得更好，就必须对区块链的性能进行改进，采用分层架构、侧链技术、闪电网络等方法来提高区块链的交易处理速度和吞吐量，并且还可以采用分布式存储和缓存技术来提高数据访问速度。

4.1.3 加强安全防护

虽然区块链本身就有一定的安全性能，但是仍然需要加强安全防护。可以利用防火墙、入侵检测系统、加密算法等技术给区块链系统提供安全保护。同时还要定时对系统实施安全评定及漏洞探测，及时找出并改正安全漏洞，保证系统安全运行[4]。

4.2 管理层面

4.2.1 建立完善的管理制度

为了保证区块链在社保卡一卡通数据安全及隐私保护中有效的使用，必须要有完整的管理措施。例如数据访问管理制度、密钥管理制度、安全审计制度等。通过制定各项管理制度来规范系统操作流程，加强对系统中数据的安全和隐私的管理。

4.2.2 加强人员培训

区块链技术属于新兴技术，相关人员的知识技能水平直接决定系统应用效果，因此要加大对系统管理人员、开发人员和使用者的培训力度。培训内容有区块链技术原理、应用场景、安全防范等，经过培训提升员工的专业素质和安全意识，保障系统的安全运行。

4.2.3 加强监管与合作

社保卡一卡通系统牵涉的部门机构很多，要加强监管合作。监管部门要制定相应的政策、标准，规范区块链在社保卡一卡通系统中的应用，各部门、机构之间要互相配合、共享数据资源，共同促进社保卡一卡通系统的安全发展。

5 案例分析

5.1 某地区社保卡一卡通系统应用区块链的情况

某地社保卡一卡通系统用区块链解决数据安全与隐私保护问题。该地区选择以太坊区块链平台，构建起一个分布式社保卡一卡通数据管理系统。对数据采用分布式存储和加密存储，将个人敏感信息分成若干份，分别存储在不同的节点上，同时对数据实施加密。数据传

输上采用 SSL/TLS 协议以及点对点传输方式，保证数据传输过程中的安全[5]。数据访问控制上用基于属性的访问控制、智能合约来自动执行访问控制。在隐私保护上，用零知识证明和同态加密技术来保护个人隐私。

5.2 应用效果分析

应用区块链技术让这一区域的社保卡一卡通系统数据更安全、隐私更好得到保护。系统运行过程中没有出现数据泄露或者篡改的情况，保证了用户信息的安全以及用户的合法权益。用户对于自己个人隐私保护的满意程度有所上升，对于该系统本身的信任度也提高了一些。同时利用区块链的分布式架构提升系统性能，业务办理速度更快，系统更加可靠，为社保卡一卡通的推广使用打下良好基础。

6 结论与展望

6.1 结论

本文详细剖析了区块链技术在社保卡一卡通数据安全及隐私保护方面的应用可能性，研究显示，区块链依靠去中心化、无法更改、能够追踪以及智能合约等特性，能很好解决系统当前的数据泄露问题，篡改风险以及侵犯隐私等情况，在借助区块链手段提升系统的安全性与可信度后，对数据存储过程，传输阶段乃至访问控制环节都起到关键作用。

6.2 展望

将来区块链技术不断发展，它同人工智能、大数据这些前沿科技的融合应用会越来越紧密，社保卡系统智能化程度和服务效率也就会相应提升，这时要同步开展相关标准创建和合规监管工作，保证技术能够规范且安全地被使用，当社保卡的功能以及涵盖的范围持续扩大时，区块链也许会在更多社会保障场景中发挥作用，帮助公共服务体系实现数字化转型并改善其质量。

参考文献

[1]段鹏飞.基于区块链的敏感数据受控安全共享及隐私保护技术研究[D].北京邮电大学,2025.

[2]陆宇锴.基于区块链技术的数据安全与隐私保护系统设计应用[J].信息与电脑,2025,37(05):62-64.

[3]姜正涛,鄢智琛,彭逸阳,等.区块链数据隐私保护关键技术与应用[J].保密科学技术,2025,(01):27-33.

[4]朱金玉.区块链技术在网络安全与隐私保护中的应用探索[J].中国宽带,2024,20(10):115-117.

[5]张旭辉,杨新涛,方有轩,等.基于区块链技术的数据安全与隐私保护机制研究[J].中国宽带,2024,20(09):28-30.