区块链技术在个人金融信息隐私保护中的运用研究

陈　序
苏州数桐数字科技有限公司，中国·江苏　苏州　215000

【摘　要】在当前的金融环境背景下，要想对个人信息隐私进行充分的保护，就要引进更加先进的技术。目前区块链技术已经广泛应用与这一领域中，且技术的应用优势比较明显。在进行区块链技术应用时，需要在掌握技术应用特点的基础上，对技术的应用形式进行正确的选择。目前区块链技术主要存在不可篡改和加密算法以及去中心化等特征，可以通过这项技术的应用，可以降低个人隐私风险。本文就区块链技术在个人金融信息隐私保护中的运用进行相关的分析和研究。

【关键词】区块链技术；个人金融信息隐私保护；运用；分析研究

在当前的时代背景下，信息化技术的发展速度正在不断的加快，个人的金融信息安全，也引起了社会各界的广泛关注，因为个人的金融信息与个人财产之间存在密切的联系，一旦信息数据遭受侵犯，就会降低个人的财产应用安全，而且信息的泄漏，会对整个行业的发展产生不良影响。目前在对个人金融信息安全进行保护时，已经应用了一些新型的信息化技术，其中的区块链技术在应用时具备更好的效果。例如可以采用分布式的账本技术，对用户的交易信息进行全面的记录，且记录形式存在开放透明和不可篡改等技术特征[1]。

1　区块链技术在个人金融信息隐私保护中的应用措施

1.1信息保护授权策略

在对个人的金融信息进行使用授权时，主要采用了应用型的授权模式。每一个用户对于信息的授权，都属于特定的应用，每次应用都存在特定的目的和使用方式以及使用期限、使用时可能带来的风险，这些使用信息会通过区块链技术，采用智能合约的形式生成合约代码。在进行应用创建时，需要通过用户进行授权，授权之后可以得到特定的IP，每个IP存在一个不同的公约，可以对使用双方的责任和义务进行明确的界定。用户可以通过这个ID，对授权情况进行实时的查看。如果存在超越了权限的用户，可以取消授权。这项应用的创建，本质是为用户信息的使用提供技术准则，满足相应的要求之后，才能开展授权工作。在进行授权的过程中，还存在一定的风险，用户要对这些风险存在明确的认知，并且存在随时取消授权的权益[2]。

在进行授权时，用户存在信息的应用权。在授权应用时，所以选择授权，也可以选择停止授权。用户的每一次授权，都存在区块链的记录。在进行应用创建时，个人信息的使用者和用户之间存在合约。合约对所有的信息进行了明确的规定，一旦在进行应用使用时，存在了违规现象，用户需要取消授权。用户可以通过授权，向使用者发送经过加密的个人信息，使用者可以通过ID接收信息，并且得到使用的授权。每次授权时，都存在使用记录。应用完成之后，用户可以通过加密信息的发布，对区块链上的信息进行更新，应用完成之后可以取消授权，使用者无法再访问相应的信息。在进行应用使用时，存在主动通知和主动查询以及知情举报违约等功能。用户存在信息的使用知情权，使用者在使用信息时，应用会将信息的使用情况和存在的风险以及信息的完成情况主动告知用户，用户也可以主动查询相应的信息。在进行信息查询时，使用者需要在一定期限内回复，否则视为侵权。用户的信息加密之后，可以储存在区块链中，每一次授权的应用信息，都会公布在区块链中。一旦存在异常数据信息，区块链可以通过举报机制，将这一异常情况反馈给用户，用户可以立即停止授权。如果存在被多次举报的使用者，信用度会不断下调，并且在区块链中公开[3]。

1.2信息保护控制策略

在对个人金融信息进行控制时，首先要做好信息的登记和确权，要明确信息的所有权。用户拥有信息的所有权，在对个人金融信息进行保护时，主要是对用户的权利进行保护。如果存在侵犯个人信息的行为，可以将其判定为个人权益的侵犯。银行等金融机构在进行金融交易时，属于信息的保管者。在进行信息使用时，仅限于用户交易活动中，不能用作其他领域。在对个人的金融信息进行确权时，可以通过区块链中的数字签名算法，采用公钥和私钥对信息进行控制。在对信息进行保护时，因为区块链属于开放性的环境，为了防止信息被其他人利用，需要通过加密储存的方法，对信息进行全面的保护[4]。

1.3信息储存策略

在进行个人金融信息储存的过程中，需要采用去中心化的储存方式，这项方式也是区块链技术的应用特点之一。在进行技术应用时，可以将加密之后的个人金融信息数据保存到区块链的节点上，避免个人的金融信息数据出现丢失和被篡改等问题。即使某一个节点的数据信息发生了问题，也不会对整体的数据储存产生不良影响。在进行去中心化区块链建设时，个人信息的掌控权，属于具备权限的用户个人，用户不仅具备修改的权限，还具备加密的权限。在进行信息数据应用时，也不会受到金融机构的影响。一旦个人的金融信息出现了变动情况，用户可以通过加密权限和解密权限，对数据信息进行有效的修改，并且在区块链中进行加密的发布。各个节点的数据信息，要通过用户的数字签名，才能实现同步的更新，这就保证了个人的金融信息在使用时，不会为某一个金融机构掌控和窃取，进一步提高了个人的金融信息储存可靠性和准确性[5]。

1.4信息的防泄漏策略

因为区块链属于开放性的环境，为了防止在区块链上，保存的个人金融数据信息被他人利用，可以对相关的数据信息进行加密储存，只有用户可以通过私钥，对相关的数据信息进行访问和编辑，因为用户的数据信息被储存在区块链中，通过加密的形式进行管理，银行等金融机构在访问信息时，需要通过用户的授

权，才能实现各项操作，在访问期间只能进行数据信息的浏览和阅读，不能对其进行复制和篡改，用户个人在对金融机构进行授权时，可以通过个人的私钥与金融机构的公钥进行匹配，完成数据信息的查看，并且生成加密的密码。这个密码能够保障信息数据在授权的过程中被二次加密，用户可以通过授权，对密码进行解密或加密处理，进一步提高了数据信息的应用安全性，可以防止数据信息在使用的过程中出现泄漏等情况[6]。

2 区块链技术在个人金融信息隐私保护中的应用前景

在对区块链技术进行创新性研发时，要想拓宽这项技术的应用范围，首先要明确个人的金融信息产权，还要强化金融机构的自律，并且对现有的区块链技术进行持续的优化和完善，确保技术在使用时，能够发挥更大的作用。政府要提高对这项技术的重视程度，加大资金的投入力度，为技术的研发提供有效的资金支撑。可以将这项技术与其他的信息化技术进行有效融合，通过综合技术的使用，进一步提高技术的应用水平[7]。

2.1明确信息产权

在当前的时代背景下，数据信息的应用价值正在不断的提高，个人信息被泄露的基本原因是因为产权不够明确。一些信息数据属于个人的财产，但因为产权不明确，导致个人的信息成为了金融机构的资源。金融机构违背个人意愿，对数据信息进行商业利用，提取了信息中的商业价值，这属于违法的行为。我国政府要制定相应的法律条例，对个人金融信息的产权进行明确的规定，通过对私有产权进行界定，使得产权的判定更加清晰。如果存在个人金融信息带来的收益，要判定为个人所有，只有这样才能降低金融机构泄露个人金融信息的几率。在对私有产权进行保护时，存在相关的法律要求，金融机构使用个人信息时，如果未经个人授权，就要对其进行严厉的惩罚[8]。

2.2加强技术的研发

因为区块链存在公开性的特征，在对区块链中的信息数据进行管理时，是通过链条的节点进行开放处理的，这就导致信息数据在储存和保护方面存在一定的问题，区块链的分布式账本结构，保证了所有录入数据信息的真实性，各个节点之间的通信，是通过密钥的验证进行处理，但因为区块链中缺乏控制节点的中枢枢纽，各个节点之间的联系，是通过信用授权或担保处理的。外部工作人员持有私钥，就可以对各个节点的数据信息进行访问，在对区块链中的加密技术进行创新性研究时，要提高信息的保护力度，通过对信息储存基础技术进行研发，确保每个节点的储存信息不能被篡改。在对传统的数据库系统进行更新时，需要增强系统的外部防控能力，在区块链的系统数据库中，即使某个节点遭受了黑客的攻击，也不会对数据信息的使用产生不良影响。即使黑客对所有的节点进行攻击，区块链技术也可以对数据信息进行快速的备份，并且生成新的节点，因此要加强节点储存技术的研究[9]。

2.3强化金融机构的自律

个人在办理金融业务时，要通过金融机构开展各项活动，在此期间会产生个人的金融数据信息。个人在参与相关交易、办理业务时，金融机构需要对个人的金融信息进行全面的保护，并且对信息数据的应用情况进行有效的监管，才能降低信息泄露和数据遗失等问题的发生几率。金融机构要想提高数据信息的监管力度，就要对内部工作人员进行专门的培训和教育，提高工作人员的风险意识。在对工作人员进行入职培训时，需要将风险防控意识和岗位风险等内容，融入到培训的各个环节中，确保工作人员能够认识到相关问题的重要性。在进行日常培训时，还需要根据岗位的具体要求，对其进行专业技能的培训和教育。例如要提高工作人员的操作水平，确保工作人员能够应该按照自身岗位的职能要求进行标准作业，尽可能降低人工失误问题的发生几率。在对用户信息进行使用时，也要严格按照程序的要求进行正确的操作，避免出现违规作业等行为，引发金融风险。因为在进行数据信息管理时，存在一定的风险问题，因此工作人员要掌握更加先进的风险防控技巧。在对个人的金融信息数据进行使用时，需要做好用户的授权管理，并且根据用户知情权的要求，做好各项问题的处理。在对内部监督审查机构进行完善和优化时，需要做好数据信息的使用记录，并且对使用情况进行全面的审查，一旦发现存在异常数据信息，要及时向用户反馈。金融机构还要构建完善的内部审查机制，要对内部各项工作的开展情况进行定期的审查，同时要对用户的投诉和反馈进行全面的分析，根据相关内容对工作人员进行科学的评价，确保工作人员的工作行为能够符合我国法律要求，工作人员还要积极的学习一些新型的知识和技术，提高区块链技术的应用熟练度，才能降低各项问题的发生概率。

3 结语

综上所述，在对个人信息进行保护时，需要对信息的来源和走向进行全方位的追踪，在进行区块链技术应用时，可以满足相应的要求。目前这项技术在应用时，可以对行业发展过程中的信息隐私保护等问题进行有效的解决。将区块链技术与个人金融信息隐私保护工作进行有机结合，可以进一步提高保护工作的开展效率，且这项技术在使用时。还可以降低个人信息的泄露风险。可以利用这项技术，拓宽个人金融信息隐私的保护思路，营造更加安全的信息环境。

参考文献：

[1]支凤稳,云仲伦,张闪闪.基于区块链的个人科学数据共享模式研究[J].现代情报,2021,41(12):69-78.

[2]邢张睿.区块链技术下公共借阅权的创新驱动发展研究[J].湖北经济学院学报(人文社会科学版),2021,18(12):85-91.

[3]秘浩.智慧城市安全体系中个人信息安全的风险与防范[J].智能建筑与智慧城市,2021(11):140-142.

[4]王真真.区块链技术在个人金融信息隐私保护中的应用[J].财会通讯,2021(14):150-153.

[5]常景超,赵蕾,李成君.金融科技背景下的隐私信息保护[J].青海金融,2019(12):31-36.

[6]王晨旭,程加成,桑新欣,李国栋,管晓宏.区块链数据隐私保护：研究现状与展望[J].计算机研究与发展,2021,58(10):2099-2119.

[7]陈晓红,张威威,易国栋,唐湘博.新一代信息技术驱动下资源环境协同管理的理论逻辑及实现路径[J].中南大学学报(社会科学版),2021,27(05):1-10.

[8]韩兴国.数字经济时代下金融科技监管体系研究——来自欧盟的监管启示[J].技术经济与管理研究,2021(09):75-79.

[9]王昱兴,袁博.从大数据杀熟到隐私泄露:软硬件视角下隐私问题的伦理分析与思考[J].科学·经济·社会,2021,39(03):72-81.