doi:10.6041/j.issn.1000-1298.2021.11.018

基于区块链的畜牧养殖资产监管身份认证研究

杨信廷[1,2]　王杰伟[1,2]　邢　斌[2,3]　罗　娜[2,3]　于华竟[1,2]　孙传恒[2,3]

(1.上海海洋大学信息学院,上海 201306;2.国家农业信息化工程技术研究中心,北京 100097;
3.农产品质量安全追溯技术及应用国家工程实验室,北京 100097)

摘要:针对畜牧养殖资产监管系统数据采集源头设备不可信,牲畜个体身份标识识别复杂,养殖敏感数据机密性差等问题,提出一种基于区块链技术和聚合签名算法的畜牧资产身份认证方案,实现资产监管系统中数据采集源头、数据存证展示的全流程真实可信,以及监管系统各节点、各物联网设备间身份验证的可信可溯,有效保障了畜牧资产监管系统从区块链网络到节点及物联网设备间细粒度的身份验证。在此基础上对方案进行混淆性分析和通信数据量分析,结果表明,加密过程的扩散性测试密文改变率平均为 93.61%,相关性测试密文改变率平均为 93.28%,具有较高的混淆性,并将通信量由线性级降低为常量级,验签耗时平均节省 40.01%,有效降低数据传输通信量和系统验证开销,具有高效的批量身份验证性能,满足畜牧资产监管过程中设备身份认证需求。

关键词:畜牧养殖;畜牧资产监管;身份认证;聚合签名;区块链;敏感数据加密

中图分类号:TP311.1　　**文献标识码**:A　　**文章编号**:1000-1298(2021)11-0170-11　　**OSID**:

Identification of Animal Husbandry Assets Supervision Based on Blockchain

YANG Xinting[1,2]　WANG Jiewei[1,2]　XING Bin[2,3]　LUO Na[2,3]　YU Huajing[1,2]　SUN Chuanheng[2,3]

(1. *College of Information Technology*, *Shanghai Ocean University*, *Shanghai* 201306, *China*
2. *National Engineering Research Center for Information Technology in Agriculture*, *Beijing* 100097, *China*
3. *National Engineering Laboratory for Agri-product Quality Traceability*, *Beijing* 100097, *China*)

Abstract: In order to solve the problems of distrust source of animal husbandry supervision data, complicated identification of livestock, and poor confidentiality of sensitive breeding data, an identity authentication scheme based on blockchain technology and aggregated signature algorithm was proposed to ensure the authenticity of the data source and the transmission safety. The identity authentication trust between blockchain nodes and sensing devices was realized, and the fine-grained identity examination from the blockchain network to the nodes and downstream access devices was guaranteed, so as to complete the traceability of identity of access devices on and off the chain of blockchain system. This scheme can complete the identity verification of the equipment and solve the problems of complex individual identification of equipment and difficulty in the asset supervision. The security of the authentication scheme was analyzed. The results showed that the average change rate of the diffusion test ciphertext was 93.61%, and the average change rate of the correlation test ciphertext was 93.28%. In addition, the scheme had efficient batch authentication performance. By dynamically aggregating and forwarding the signature data, the traffic was reduced from linear level to constant level, and the signature verification time was saved by 40.01% on average. It can effectively reduce the data transmission traffic and system verification overhead, and meet the needs of equipment authentication in the process of animal husbandry supervision.

Key words: livestock farming; animal husbandry assets supervision; identification; aggregate signature; blockchain; sensitive data encryption

收稿日期:2021-05-31　修回日期:2021-08-22

基金项目:国家自然科学基金项目(31871525)和北京市农林科学院科技创新能力建设专项(KJCX20210408)

作者简介:杨信廷(1974—),男,研究员,博士,主要从事农产品智慧供应链研究,E-mail:yangxt@nercita.org.cn

通信作者:孙传恒(1978—),男,研究员,博士,主要从事农产品追溯技术研究,E-mail:sunch@nercita.org.cn

0　引言

畜牧业已连续多年占农林牧渔业总产值四分之一以上，并仍有逐年增加的趋势[1]，具有广阔的市场规模和产业前景。畜牧保险作为畜牧业发展的有效风险管控工具，已成为降低活畜养殖风险的重要手段[2]。随着规模化、信息化的集约养殖模式发展，构建资产监管系统保障活畜资产可查可控是确保畜牧保险投资安全的重中之重。监管系统需要实现对牲畜的良好监控，准确获取牲畜生长数据及环境信息等要素用以保障资产审查[3]。

对于畜牧养殖企业中心化的管理结构，保险、银行等金融机构难以对其完全信任，尤其涉及投保业务时，养殖数据的真实性、有效性无法保障[4]。区块链技术以其不可篡改、分布式、强共识的特性[5]，可以有效保障资产监管系统追溯数据真实性及可用性[6]。基于区块链技术的资产监管系统，实现对牲畜状态的良好监控及资产审查，并借助区块链高可信性的技术特点，完成对监管数据可靠性的有力保障[7]。其中，文献[8]提出一种基于区块链技术的畜牧养殖管理系统，规划牲畜养殖信息并对养殖环境追溯，为牲畜养殖提供优化方案增加养殖产能。文献[9]对以区块链技术驱动养殖业保险的发展进行了研究，利用区块链技术不可篡改、强共识、去中心化等特征，构建基于区块链技术的养殖业数据溯源监管系统，从饲养、防疫、育肥、出栏等阶段记录养殖数据，对于银行业查验牲畜数据，保障活畜资产监管具有重要价值。但当区块链网络有效保障养殖数据的信息安全性及可信性后[10]，用于获取牲畜生长状态信息的传感器设备安全性仍缺乏有效控制，在监管系统数据来源端其数据完整性、机密性、可用性无法得到有效保障。区块链监管系统的安全性仅能保障到区块节点级，对于养殖场中所引入的大量传感器监测设备缺乏有效的安全检验手段。故而，有必要对监管系统数据来源真实性进行鉴别和安全检测。

牲畜个体信息和行为智能感知是精准畜牧业的核心[11]，是资产监管系统可用的必要条件。资产监管系统通过个体识别技术获取牲畜的生长状态，从而具有可靠的金融监管应用价值[12]。在对牲畜进行个体标识获取牲畜生长状态的研究中，文献[13]对于奶牛养殖过程，提出了基于射频识别技术(Radio frequency identification，RFID)的身份识别系统标识牲畜个体，使用瘤胃式动物电子标识为奶牛建立数字档案。但该方案对标签硬件要求较高且不具有安全识别认证模块，对于设备身份冒名及数据机密性缺乏保障。基于植入式 RFID 芯片的牲畜体温监测及身份标识大范围应用成本较高，且固定式 RFID 阅读器不具有灵活性[14]。文献[15]对于牛只身份识别方式进行了研究，结果表明耳纹、热铁烙印、无线射频识别等身份识别方式具有标记欺诈、工作重复、监测成本高等不足，其认为牲畜面部识别的非接触式身份识别具有良好前景。但对于中小规模养殖场，牲畜面部识别具有较高使用成本且无法对牲畜生长状态进行数据监测，牲畜养殖数据亦缺乏机密性保护，文献[16]基于卷积神经网络的奶牛个体身份识别方法也具有同样问题。以上研究可以实现对牲畜个体生长情况的有效监控，但缺乏对终端设备身份的验证审查，无法完成监管系统数据采集源头的真实性检验，无法保障养殖数据传输过程的机密性、有效性。

保障终端传感器数据来源真实有效，保障数据采集设备全流程可信是资产监管系统可信可用的首要条件。使用 RFID 等传感器设备可以实现对活体牲畜个体的有效识别，但当传感器设备接入系统时，如何确保接入设备的可信性，杜绝设备身份冒名、信息篡改等物联网设备自身具有的安全隐患[17]，确保监管系统采集的源头数据真实可信是需要解决的问题。身份识别认证可以有效检验数据来源真实，保障数据采集端来源可溯，作为资产监管系统整体安全性的第一道屏障，可对设备进行有效的身份核验，仅允许登记授权的设备接入网络，维护终端设备可信性。依托区块链技术，从区块链网络及实体节点到物联网设备间细粒度的身份标识可溯，对于构建资产监管系统全流程真实可信具有重要的现实意义。

针对以上情况，提出一种基于区块链的畜牧养殖资产监管身份认证方案。对于畜牧养殖中牲畜身份识别及监管系统数据来源不可信问题，通过身份认证方案为数据机密性及设备身份可靠性提供有效支持，实现区块链畜牧资产监管系统的细粒度身份标识。以基于区块链技术的畜牧资产监管系统实现对牲畜个体的有效监管，通过传感器设备实时监测牲畜个体健康状况，以期实现对活畜资产的动态评估审核，防范畜牧保险承保风险。

1　基于区块链的畜牧养殖资产监管模型设计

1.1　畜牧养殖资产监管业务流程

在畜牧养殖过程中，由于存在活畜资产授信贷款困难、抵押不可信等问题，畜牧企业(牧企)希望盘活牲畜资产，通过活畜抵押方式进行贷款融资，扩大养殖规模，将面临严峻挑战[18]。因此构建资产监

管系统帮助牧企实现资产可信,帮助银行实现可靠抵押具有重要应用价值。银行业希望借助资产监管系统实现在贷款行为中对牲畜状态的实时监管,进行资产审查,降低活畜信贷风险。以区块链技术为基础的畜牧资产监管系统,借助其不可篡改性、强共识特性保障数据高度可信[19-20],实现相关实体的共同参与与监督,确保牲畜的良好生长。

资产监管系统的主要参与实体为养殖户/养殖企业、保险公司、银行及信息技术服务商等。利用该系统金融参与者可通过牲畜运动信息监督牲畜存活状态,对资产进行评估监测,确保牲畜处于可抵押的良好状态,并监督查看养殖户的饲养行为,规避逆向选择风险;养殖企业可以实现资产盘活获得贷款,为其养殖生产行为提供资金支持。通过该监管系统的信息整合及实时查验,可有效帮助多方间实现信息共享并以高度的可信性、不可篡改性实现对活畜资产的有效管理。

本文设计的区块链畜牧资产监管模型面向养殖监管过程如图 1 所示。其中养殖户/牧企、保险公司、银行、监管部门作为实体节点加入区块链网络,并完成对养殖数据的区块链存证写入,实现节点间对养殖信息的数据共享,使得各参与方实体均能够实时查看牲畜状态数据并进行有效监管。当养殖户与保险公司建立承保关系或与银行建立贷款关系时,相关方可实时审查畜牧资产的生存状态,动态评估资产存活风险,并进行资产数据监管、信贷监督、数据确权等行为,当发生牲畜疫病或牲畜死亡时,系统触发智能合约养殖保险条约,保险公司、银行可通过线上审查、实地再核实等手段展开对养殖户的理赔工作,进行相关业务操作。

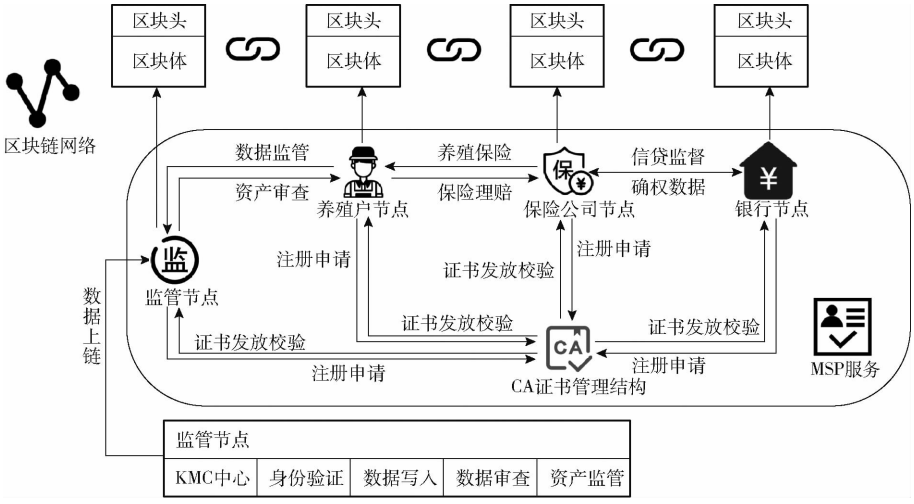

图 1 区块链畜牧资产监管模型

Fig. 1 Blockchain animal husbandry asset supervision model

1.2 资产监管身份认证方案设计

区块链技术具有不可篡改、去中心化的技术特点,对监管系统可信性提供了有效的信用背书[21]。基于区块链的资产管理身份认证方案流程如图 2 所示,主体内容由区块链网络初始化节点准入、设备端身份验证、区块链节点身份验证 3 部分构成。在区块链网络初始化阶段,以 Fabric-CA 完成对系统初始化时养殖户/牧企、保险公司、银行、监管部门等实体的申请批复、身份证书发放等工作,并对节点准入进行审核,由成员关系服务提供者(Membership service provider,MSP)服务对节点权限和身份进行划分,由于实体节点参与程度及各方利益差异,其数据操作权限将存在不同的划分方式。完成网络初始化及节点加入后,将进入设备端身份验证阶段。该部分由数据采集、数据加密、数据签名、签名聚合、签名验证操作构成。系统初始化完毕后,传感器设备将通过感知传感器等元件进行数据采集,并对采集数据进行加密签名操作,实现传感器设备与密文数据包的唯一对应标识。设备端将对密文数据及签名打包发送给上层设备,由上层设备完成签名聚合操作,并将聚合结果发送给区块链验证端监管节点实现设备端身份验证。在区块链节点身份验证阶段,监管节点获取数据后,通过区块链共识机制完成数据上链实现数据在网络中多节点共享,该过程网络仍对上链监管节点进行身份验证,以保证该节点的身份可信性。以此,达到对网络系统中准入节点、接入设备的细粒度身份审查,实现资产监管系统全流程数据可信。

监管系统所使用的区块链网络以 Hyperledger Fabric 为底层框架,在区块链网络初始化节点准入阶段,系统对加入节点进行身份验证保障其身份可信。当养殖户/牧企、保险公司、银行、监管部门等实体作为节点初始化加入网络时,须向证书颁发机构(Certification authority,CA)提交申请注册请求,由

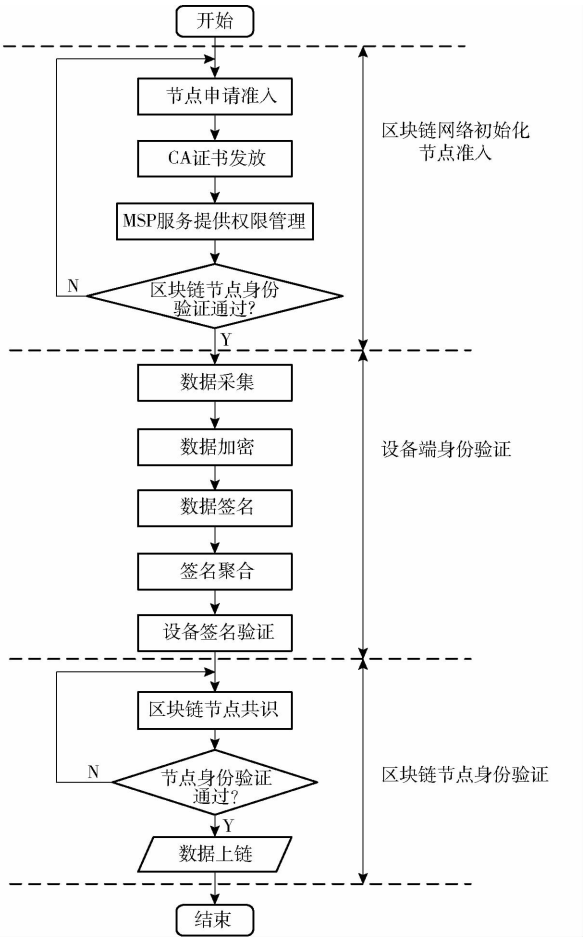

图 2　认证方案设计流程图

Fig. 2　Authentication scheme flow chart

CA 向节点颁发身份证书，并颁发为保障通信安全而准备的安全传输层协议（Transport layer security，TLS）证书，用于安全通信会话操作，该证书均为 X. 509 标准格式。当 Fabric－CA 生成证书及密钥后，即完成了对 MSP 服务的初始化操作，CA 作为 MSP 服务接口的实现方式，完成对节点及各组织间的身份定义、身份验证管理、签名校验等操作。网络对注册申请加入的节点身份验证过程如图 3（图中，CA1. 1 表示监管节点 1 所拥有的认证证书，CA1. 2 ~ CA4. 2 类同）所示。由 MSP 服务抽象提供对节点、网络、组织间的验证核实工作。节点使用椭圆曲线数字签名算法（Elliptic curve digital signature algorithm，ECDSA）利用自身身份证书生成签名，该值绑定到特定标识的字节数据。验证算法将 CA 证书身份、认可（由 CA 输出）、签名作为输入，若签名与认可的有效签名一致，则输出“accept”，否则输出“reject”。当为“accept”时，用户节点可以看到网络事务并与网络中的其他参与者执行事务，若为“reject”，则表示用户节点未经过身份验证，无法向网络提交事务或行使其他操作权限。

针对区块链网络初始化节点准入及数据上链时区块链节点共识身份校验，通过 CA 证书校验模式完成节点身份验证。当节点申请准入并通过 MSP 服务获得相应权限后，单个实体的 CA 证书均包含其身份信息，通过证书校验实现节点间身份标识。区块链网络对于监管节点数据上传操作仍将通过 CA 证书完成对监管节点的数据上链身份验证，保证每次数据上链时节点身份均不存在伪造。

节点通过验证加入到区块链网络中后，将进行对系统接入的物联网传感设备的身份审核。针对设备端身份验证阶段，以区块链监管节点实现对物联网传感设备的身份验证。在数据传输之前，对发起数据传输请求的设备进行身份认证，通过监管节点公钥对采集数据加密，保证数据仅以密文形式被监管节点查看。传感器设备对密文数据签名，并将密文数据及签名数据发送给监管节点实行身份校验，实现信息的机密性保护及设备身份审查。通过窄带物联网（Narrow band internet of things，NB－

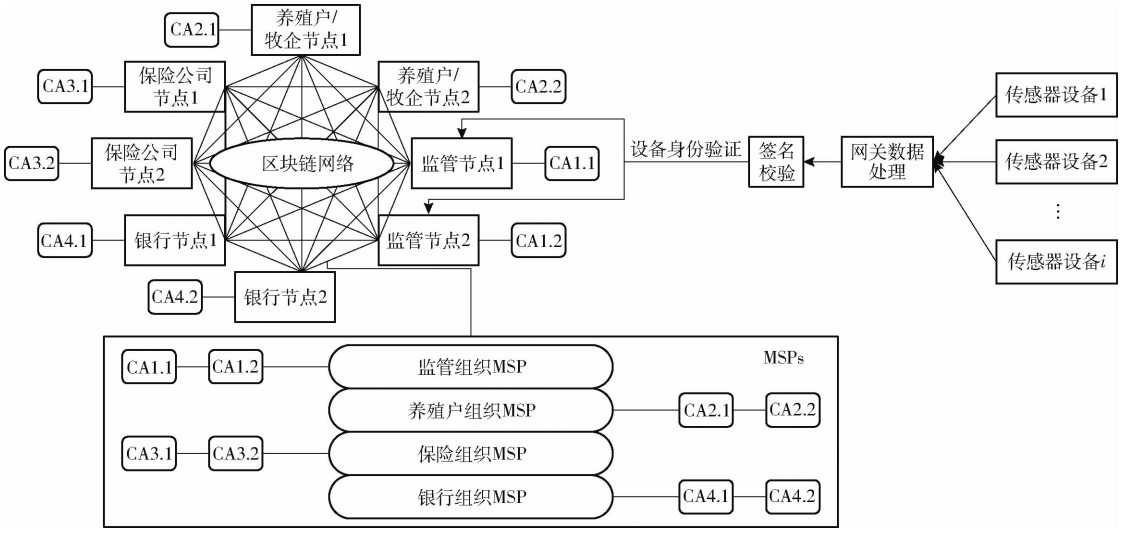

图 3　区块链节点身份验证方案

Fig. 3　Blockchain node authentication scheme

IoT)[22]、蓝牙等通信技术将数据发送给网关路由，经其聚合转发给监管节点进行区块链数据存证。实现区块链网络存证到节点与传感器设备间均完成身份验证，并通过加密算法，避免明文传输带来的信息泄露、数据篡改等问题。

设备端身份验证过程主要分为：①参数初始化、密钥生成、广播（其中包括加密密钥对、签名密钥对）。②传感器设备数据加密、签名。③网关设备数据存储、转发、聚合。④节点验证端身份验签等步骤。设备端身份验证具体流程为：

（1）由密钥管理中心（Key manage center，KMC）根据本方案使用的加密算法 SM2 及签名算法 BLS 进行参数初始化并生成加密密钥对、签名密钥对：①根据加密算法 SM2 初始化加密椭圆曲线。②输入一个有效的有限域 F_q 上的椭圆曲线参数集合，输出与椭圆曲线系统参数相关的一个密钥对(d,K)，该对密钥由验证端持有，其中 d 为加密私钥，K 为加密公钥。③根据 BLS 聚合签名算法初始化一个质数阶双线性群。④由质数阶双线性群生成签名私钥 P_k 和签名公钥 P，该密钥对数量与传感器设备数量一致。

（2）由 KMC 将加密私钥传递给验证端节点，加密公钥广播给各参与方。将签名私钥传递给每个传感器设备端，签名公钥进行广播。

（3）第 $i(1\leqslant i\leqslant r,r$ 为传感器设备总数）个传感器设备采集数据 m_i 之后，使用验证端加密公钥 K 对其进行加密，随后使用该设备自身的签名私钥 P_{ki} 对密文数据进行签名，即：①对明文数据信息使用 SM2 算法做加密运算，$C_i=E_{\mathrm{SM2}}(m_i)$。②利用密文消息进行曲线哈希计算，得 $H(C_i)$。将 $H(C_i)$ 与该设备的私钥作曲线点乘计算得签名 $S_i=S_{\mathrm{BLS}}(C_i)=P_{ki}H(C_i)$。

（4）第 i 个传感器设备将密文数据 C_i、密文曲线哈希 $H(C_i)$、签名数据 S_i 发送给网关。

（5）网关收到所有传感器设备发送的数据对 $C_i+H(C_i)+S_i$，并对所有设备的 $H(C_i)$ 和 S_i 进行密文哈希聚合及签名聚合操作，即

$$\sigma(H)=\sum_{i=1}^{r}H(C_i) \tag{1}$$

$$\sigma(S)=\sum_{i=1}^{r}S_i \tag{2}$$

式中 $\sigma(H)$——所有传感器设备密文曲线哈希聚合后的值

$\sigma(S)$——所有设备签名数据聚合后的值

该聚合运算为椭圆曲线上的点加运算。随后，将 C_i、$\sigma(H)$、$\sigma(S)$ 发送给验证端区块链节点。

（6）验证端节点收到 $C_i+\sigma(H)+\sigma(S)$ 后，进行验签判断。

将设备各公钥进行聚合

$$\sigma(P)=\sum_{i=1}^{r}P_i \tag{3}$$

式中 P_i——第 i 个设备的签名公钥

$\sigma(P)$——所有设备的公钥聚合值

通过双线性对运算判断等式 $e(\sigma(P),\sigma(H))=e(G,\sigma(S))$ 是否成立（其中，$e(x,y)$ 表示对 x、y 做双线性对运算，G 为 BLS 算法初始化中椭圆曲线生成点）。若等式成立，则所有传感器设备身份认证均通过，否则身份信息有误，判断单个设备身份是否合法。

区块链验证端监管节点与传感器设备端的身份验证实施流程如图 4 所示。

当区块链系统网络通过 MSP 服务及节点身份证书完成对养殖户/牧企、保险公司、银行、监管部门等实体节点的身份准入验证，并通过监管节点对传感器接入设备进行签名校验完成设备身份验证后，验证端监管节点将获取到设备端传输的养殖敏感数据，由监管节点对这些数据进行记账上传操作。该过程中节点间通过 Kafka 共识机制完成对上链数据共识，并对每一次上传过程中的节点进行身份校验，若节点证书不可靠，将重新共识，最终完成节点数据上链存证操作。

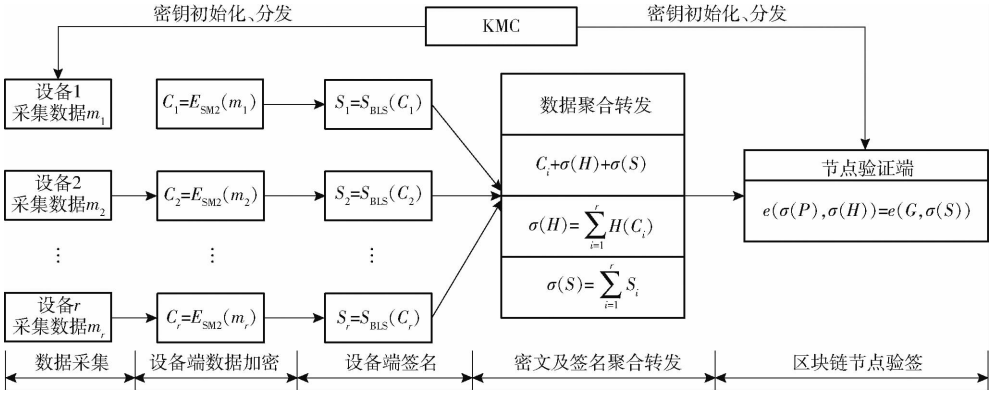

图 4 设备身份验证方案

Fig. 4 Equipment identification scheme

通过以上过程，区块链网络对申请节点以身份证书方式进行准入验证，标识每个节点的身份信息，并通过验证端监管节点以设备数据签名方式完成对接入传感器设备的身份校验。通过该身份认证方案可以有效实现区块链网络到准入节点及接入传感器设备间的细粒度身份验证，实现从数据源头采集、数据展示、数据存证到数据查验的全流程可信、可溯、可查，保障了养殖监管数据的全流程安全可靠，对于金融、承保等行为具有高度的信息参考价值，帮助相关参与方实现信息可靠共享查验。

2　畜牧养殖资产监管身份认证方案实现

在内蒙古自治区锡林郭勒盟某牛场对畜牧养殖资产监管系统进行了试点应用，完善牛场资产监管体系。通过区块链畜牧养殖资产监管系统实现对活畜资产状态实时查验，帮助养殖户、保险公司等相关参与方对牲畜生长状态进行监测，为资产审查提供数据支持。在该试点应用中，系统通过对养殖设备的身份认证及所产生数据的加密处理保证区块链监管系统数据的真实性。系统所采用的总体框架为 4 层体系结构：感知层、网络层、云服务层、业务应用层，如图 5 所示。

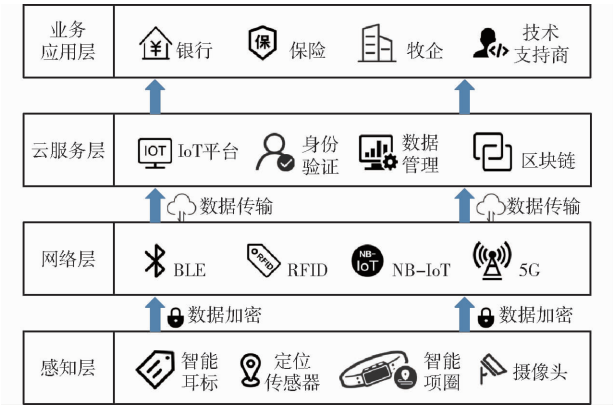

图 5　资产监管系统架构图

Fig. 5　System structure of asset supervision

感知层作为系统数据采集端，通过摄像头、定位传感器、智能耳标等进行数据采集，并将数据加密签名向上层网络传输。网络层对感知层上传的数据进行聚合转发，完成对签名数据的初步操作，并将相关数据发送给上层网络进行设备签名验证。在云服务层搭载物联网服务平台、区块链网络等，与系统融合组建畜牧资产监管系统，完成对设备端身份校验并对养殖敏感数据进行区块链存证。业务应用层面向系统使用者，作为畜牧资产监管系统的参与方，银行、保险、牧企、技术支持商等共同构建真实可信的资产管理平台，共同维护畜牧行业的发展建设，促进各方之间信息透明共享，维护良好的资产监察。

在系统试点应用中，养殖场以智能耳标作为物联网传感器终端进行数据采集。通过智能耳标监管牛只体征信息，智能耳标传输的监测参数为：畜牧编号、网关 ID、设备 ID、在线状态、牲畜种类、二级种类、性别、绝育状况、牲畜品种、养殖场景、当前状态、运动量、当前体温、身份认证、抵押到期日、售卖状态。智能耳标使用低功耗蓝牙（Bluetooth low energy，BLE）通信方式，运动量、体温等参数每 10 min 上传一次。以某一设备为例，给出其采集到的参数字段及数据信息，如表 1 所示。

表 1　设备数据详情信息

Tab. 1　Information of equipment data

序号	字段	参数值
1	网关 ID	G2303M203300018
2	设备 ID	A12301M204504876
3	在线状态	在线
4	牲畜种类	牛
5	二级种类	肉牛
6	性别	公
7	绝育状况	否
8	牲畜品种	西门塔尔
9	养殖场景	圈养
10	当前状态	育肥
11	运动量	1 068
12	当前体温	38.2℃
13	身份认证	是
14	抵押到期日	2021/06/17
15	售卖状态	否

智能耳标完成数据采集后，将使用区块链监管节点的验证端公钥对数据进行加密处理，避免数据的明文传输，并使用传感器设备端私钥对密文进行签名操作。设备端数据如表 2 所示，表中内容为对该设备分配的密钥信息及经过 SM2 加密、BLS 签名运算后的数据结果。智能耳标对采集数据进行初步操作后将密文数据、签名数据通过蓝牙通讯传输给网关设备。网关将对养殖场中所有设备的签名数据进行聚合运算以降低验签数据量和通信数据长度，聚合后通过 NB－IoT 技术发送给验证端进行设备身份验证，确定设备身份是否真实可信。

当传感器设备向验证端申请数据传输请求并通过身份验证后，监管节点收到经传感设备采集到的数据信息，通过共识机制与其他节点实现消息共享。数据上链之后通过 CouchDB 数据库存储，用于养殖敏感数据存证，如表 3 所示存证追溯数据式样，其内容以表 1 中所列设备数据详情信息为例进行操作处理，将文本信息转换为十六进制数据后经加密签名处理，其追溯信息密文、交易哈希值、区块高度、区块哈希值信息如表 3 所示。

表 2 设备身份认证详情信息

Tab. 2 Information of device identification

变量名	变量值
验证端公钥	047B71C05859244D26480C2504CABFCAB214FBF55C541665A6F23936F3942A6206E421C4760C86DB548751E5020E799B33121 2383CBFD2BB27C0E73A935C8CA79C
设备端公钥	672846296311740847983431665217832368205360186309244394627726624479836232330730051512830091138974847934642901654307250025020287288364015497554248287170021 6, 128449394524317146942112158700697252108031452099244866777195437 596900448561033056420980418763967194186332093962578041657833018513969522444232189561744532 9, 0
设备端私钥	99745366846962049518566811575762626190099716941
密文	045E08A5C1BA73DEA9E367FD1A547385A5B9662B6EA724ABB2F67A18E6C36FE9A05A4FED73CE2A919C50E6BD3F8C821BA 0A4F902557E29D0160D8D34370473F4B4FA4DBB4C15EEBF96455C467A5BF6D55E4839873F0D5B269565E5504DA92C5607D1 4006FE501209C23D26040BC73BEB2CA21D2C449370754A3D867ED42F0C1E9AD8B37E05A881AF85C13B1E304919CD7926B15 2777BEB04AFD47C833FE30487DBD7852B563E619B1F68107BB757DDE3725FC2423B24F05B337C0E611F6BFF829F3EA3BF777 81441E3060A48BCB9FA12E9B43C90702ED12F509207D74CEC18346F907A75B1E299C2D9B6B2766D595026D14E6987F2038CE 2682ECCC875E755E0485AEBAC213763091F798AD15115203A4589937470 24A93171B13D1B9DA4
签名	643590419511276567661008063449264018132560547865942464175012038107262864464058824953141872464345904488676415 5 166154438722510977388071459483728730459304936, 917219901313131040978802841261486456888457452693454341868299248 708039342850386555623378602986362169601623384830227890216948797198937023703833692134974 92, 0

表 3 存证追溯数据详细信息

Tab. 3 Information of traceability data

追溯信息密文	交易哈希值	区块高度	区块哈希值
04D0672C44E6E77494A94866922655AB6A84EF849A46448395ABCF5E876 F54C44B3427BA05E2CAD74D1916D1D39A42F7957389FAFFA43EF9BDD7 67E0C0D9A19DA97B0297558B896B4BAEA0D8A8BBA266687FE48946017 C936B500D242BFFB118EAA2649F4A81A9E6620FA49E816E51E294D0803 B70C597A72853FE5E1CEC62A0871F76294915223 12D43FEF4AC7F40603 CC3B65DE4097D72182E59008C9FA68EC71DD027169BDED1FE13912152 3D15CB6DD211A4D0BB69B5157938D62FC612681C8A87A1BAE4DC4DD8 7915B82B86888E12D1B60A9D2A3B069E4006A06DC9A1B8E75866D031C 94B5C08F5D6207502E3983E8FE8DE8DBB9378A74F523F4AB9201D0812 F884FBF21396044913503 15F4384BFE71E62545AB9B04F11D162B24A	7ae34dc7f207309bf2c 4b2ab8f21bc5c53095 bbfd13763edfc3f70cd 76e5bfb3	154650	a3d4c58f3453a5dfd43 9dcc9f3dcb720ecb296 eb888e51341eca830e 74e7231a

在监管系统试点应用的锡林郭勒盟牛场中，所使用的智能耳标及网关等硬件设备如图 6 所示，耳标内嵌多种传感装置，通过配带在牛耳上收集牲畜状态信息，进行数据采集与传输。网关设备对采集数据进行初步处理并对签名数据聚合计算，通过安全传输协议向上层监管节点发送数据包，通过智慧畜牧管理平台向用户展示存证数据。

图 6 智能耳标应用现场图

Fig. 6 Application scene of intelligent ear tags

区块链畜牧养殖资产监管系统所有使用的平台以 Hyperledger Fabric 为底层架构，其存证区块高度及相应哈希值如图 7a 所示。将智慧畜牧养殖监管平台与区块链系统端连接，畜牧养殖监管平台数据从区块链系统端获取，向用户进行数据展示，若用户对智慧畜牧养殖监管平台数据存疑，可通过区块链系统端进行数据核查，实现养殖监管数据可信。向养殖户、银行、保险等参与方展示的数据平台如图 7b 所示，通过该系统，养殖户实时监测牛只在线

(a) 区块链存证数据系统

(b) 智慧畜牧养殖平台

图 7 系统工作界面

Fig. 7 Interface of system working

状况，例如是否仍在养殖围栏内等，实现对牛只位置实时把控。保险、银行等参与者可查看牲畜在线状态，通过运动量、体温等参数判断牛只存活情况，解决抵押资产死亡而难以实时监测的问题。投保前后阶段，银行或保险公司可通过系统中检疫记录及疫苗记录等目录项查看、了解养殖户的养殖行为，评估养殖户在投保前后是否存在疫病防治减弱、环境卫生不主动提高、放弃对风险预防的努力等故意加剧承保风险的行为。通过对潜在风险洞察分析，保险、银行等金融机构可以有效规避承保风险，实现畜牧信贷产业良性循环。

3　测试与分析

3.1　困难性问题

本认证方案设计中，签名算法及加密算法所依据的困难性数学问题包括：椭圆曲线离散对数问题、质数阶双线性群运算、密钥交换协议问题等。该困难性问题保证签名算法、加密算法在数学上是理论可行的，其暴力破解是困难的。

椭圆曲线离散对数问题（Elliptic curve discrete logarithm problem，ECDLP）：已知定义在有限域 F_q（阶为 q）上的椭圆曲线，该曲线阶为 n，点 G、Q 均属于该曲线。ECDLP 是指确定整数 $x\in[0,n-1]$ 使得 $Q=xG$ 成立，以 Q 为公钥，以 x 为私钥。在该问题中 $Q=xG$ 的正向计算是简单的，反向计算由公钥 Q 破译私钥 x 是复杂的，在有限多项式时间内难以从 Q 中计算出 x 的值，该值作为基于 ECDLP 问题的非对称加密私钥是安全的。该问题对于参数的选择要求使用大素数。本方案所用加密算法基于该 ECDLP 问题，可有效保障密钥的安全性。

质数阶双线性群：由五元组 (p,G_1,G_2,G_T,e) 描述。其中 p 是一个与给定安全常数 δ 相关的大素数，G_1、G_2、G_T 是阶为 p 的乘法循环群，e 为双线性映射规则 $e:G_1\times G_2\to G_T$，该规则满足双线性、非退化性、可计算性 3 个条件，即：

双线性条件

$$\forall g\in G_1,h\in G_2,a、b\in Z_p\Rightarrow e(g^a,h^b)=e(g,h)^{ab} \tag{4}$$

非退化性条件

$$\exists g_1\in G_1,g_2\in G_2\Rightarrow e(g_1,g_2)\neq 1 \tag{5}$$

可计算性条件

$$\forall u\in G_1,\ v\in G_2,\ \exists t(\delta)\Rightarrow e(u,v) \tag{6}$$

式中　Z_p——整数域

a、b——整数域内的元素

g、g_1、g_2、h、u、v——乘法循环群内的元素

$t(\delta)$——与安全常数 δ 有关的多项式时间算法

畜牧资产身份认证方案所使用的 SM2 加密算法基于 ECDLP 问题，BLS 聚合签名算法以质数阶双线性群为数学基础，其在数学上的理论证明确保了该方案在破解过程中的困难性。使得身份认证方案中对数据的加解密操作及聚合、配对运算、签名生成、签名验证等操作均具有数学合理性及安全性。

Diffie－Hellman 密钥交换协议（DH 问题）：该问题是一种确保共享密钥在不可信网络中安全传输的方法，该机制可以在需要安全通信的双方间交换密钥信息，避免密钥分发传递时的窃听现象。其算法过程为：

（1）通信双方甲、乙事先约定算法参数：素数 p、f 分别作为模数和基数，该值可对外公开。

（2）对甲，以一个秘密的自然数 c 作为自身私钥（不公开），计算 $A=f^c \bmod p$ 作为自身公钥（可公开）。

（3）对乙，以一个秘密的自然数 l 作为自身私钥（不公开），计算 $B=f^l \bmod p$ 作为自身公钥（可公开）。

（4）甲乙双方交换各自公钥。

（5）甲计算出 $k=B^c \bmod p$，乙计算出 $k=A^l \bmod p$。甲乙完成密钥的协商，得到密钥 k。

计算 Diffie－Hellman 难题（Computational Diffie－Hellman problem，CDH 问题）：给出任意的 w、w^x、w^y，求解 w^{xy} 是困难的，该问题是指窃听者尝试计算 DH 问题，但理论证明尚不存在一个概率多项式时间图灵机能够有效地计算该问题，即破解该问题获取密钥是困难的。

3.2　正确性证明

当网关收到传感器设备传输的签名数据后，对签名数据进行无证书聚合操作，实施双线性配对运算。所得聚合签名 $\sigma(S)$ 的正确性及有效性推导过程为

$$P_i=P_{ki}G \tag{7}$$

$$S_i=P_{ki}H(C_i) \tag{8}$$

$$\sigma(S)=S_1+S_2+\cdots+S_{1000} \tag{9}$$

$$\begin{aligned}e(G,\sigma(S))&=e(G,S_1+S_2+\cdots+S_{1000})=\\&e(G,S_1)e(G,S_2)\cdots e(G,S_{1000})=\\&e(G,P_{k1}H(C_1))\cdots e(G,P_{k1000}H(C_{1000}))=\\&e(P_{k1}G,H(C_1))\cdots e(P_{k1000}G,H(C_{1000}))=\\&e(P_1,H(C_1))e(P_2,H(C_2))\cdots e(P_{1000},H(C_{1000}))\end{aligned} \tag{10}$$

$$\begin{aligned}e(\sigma(P),\sigma(H))&=e(P_kG,H(C))=\\&e(G,P_kH(C))=e(G,\sigma(S))\end{aligned} \tag{11}$$

该过程有效论证了签名算法中的聚合过程在数学上的正确性，其数据压缩结果在数学上是成立的，

聚合运算过程对签名数据量进行压缩,为提高验证效率做出了重要贡献。双线性运算由于其独特的性质使签名算法可以完成聚合操作,通过以上推导可知聚合验证过程理论成立,并具有严谨的数学支持,算法合理性经过有效证明。

3.3 混淆性分析

在密文数据传输时,非授权用户截取报文传输获取数据的方式大多为 2 种:①传输信道中通过监听抓取,对截获的密文暴力破解,由密文直接获取明文数据。②通过对密钥分发时进行定点监听,试图抓取加解密密钥对,直接对密文解密获取数据。本方案中各算法基于椭圆曲线离散对数问题[23]、CDH 问题,非授权用户难以在有限多项式时间内成功对密文数据实施暴力破解。其次求解 DH 问题是困难的,因此非授权用户亦无法实现对密钥的监听截取。因此,本文所提出的身份认证方案具有较高安全性,其安全基础来源于已证实的数学难题,其次,来源于 SM2 加密算法和 BLS 签名算法在构造过程中已证实的安全性[24]。

对于本方案所使用的加密算法 SM2,通过扩散性、相关性衡量算法混淆性,以算法扩散性及相关性作为指标可有效衡量签名算法安全性[25]。定义密文改变率 $\Delta = \lambda/\gamma \times 100\%$,其中 λ 为密文改变位数,γ 为密文总位数。在一次测算过程中,控制明文数据不变,当对密钥做出修改时所引起的密文改变率如图 8 所示,其表征的是密钥对密文扩散性的影响,扩散性的平均密文改变率为 93.61%。控制密钥数据不变,当明文改变时所引起的密文改变率如图 9 所示,表征明文与密文间的相关性,相关性的平均密文改变率为 93.28%。由此可知,该加密算法具有良好的安全性和较高的混淆性。

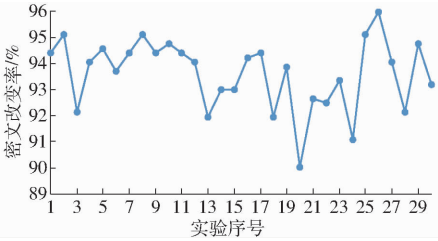

图 8 扩散性分析

Fig. 8 Diffusion analysis graph

3.4 开销分析

与椭圆曲线密码学(Elliptic curve cryptography,ECC)等非聚合签名算法相比,当大量设备端接入系统时,使用聚合签名算法可有效降低签名数据长度,有效减少信道通信量,降低验证计算复杂度,减少系统应用时间开销。对签名过程中是否使用聚合运算的签名数据长度进行对比,结果如图 10 所示,随着终端设备接入数量的不断增加,签名数据呈线性增长,而使用基于聚合签名的认证算法,签名长度可保持常量级别,不会随大量设备接入而增加通信成本。对于使用大量传感设备的畜牧养殖监管场所,该认证方案能够有效减小签名长度,有效降低签名传递通信量,在畜牧养殖的户外场所中可以有效降低不同设备间的信息通信载荷。

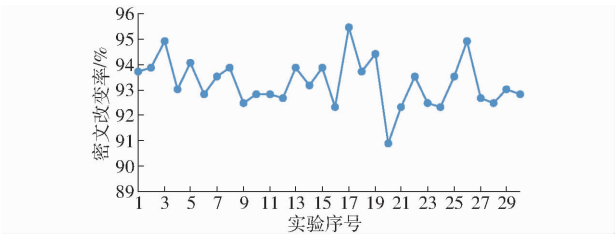

图 9 相关性分析

Fig. 9 Correlation analysis graph

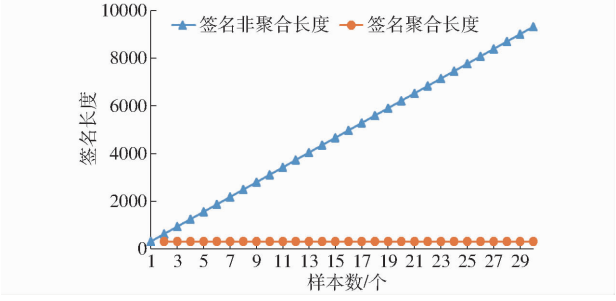

图 10 签名长度对比

Fig. 10 Comparison of signature length

时间开销测试结果如图 11 所示,当接入设备逐渐增多时,对签名数据的直接验证时间开销是聚合验证的 2 倍。随着接入设备进一步增多,聚合验证时间开销更具优势,当接入设备数为 30 时,非聚合验签时间为 471 ms,聚合验签的时间仅 237 ms,节约用时 49.68%,总体时间开销平均降低 40.01%。另外,本文方案基于无证书签名验证,相较于使用 CA 机构的签名认证方案,不涉及证书的分发、管理、销毁等操作,可有效降低服务器端的验证管理开销。因此,本方案的总计算效率具有一定的优势,尤其当面对庞大数量的设备认证请求时,本方案的验证性能更具优势,能够更易满足大量畜牧养殖所需要的设备身份认证需求。

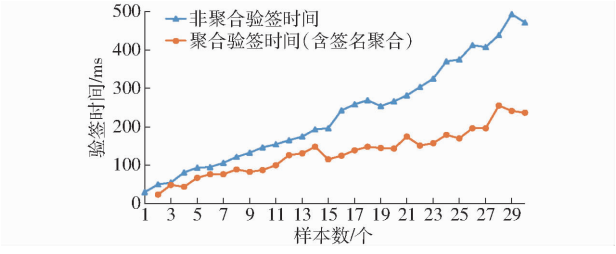

图 11 签名验证时间开销对比

Fig. 11 Comparison of signature verification time

4　结论

(1)在区块链畜牧养殖资产监管系统中,认证方案有效实现了系统内全流程、细粒度的身份审核,网络对加入节点提供了严苛的身份验证机制,保障节点身份可信,实现对区块链节点与接入传感器设备间的身份验证。通过节点与传感器设备间的身份认证及设备数据的加密运算,保障数据传输机密性、数据来源真实性,维护养殖敏感数据安全性。通过签名数据的聚合运算有效解决多方签名数据长度过长,通信量过大的问题,有效降低了签名传输长度,并保障敏感数据的密文传输,将加密、签名操作置于用户透明状态,具有良好的用户体验。最终实现监管系统数据全流程真实可信,区块链网络到节点及接入设备间的细粒度身份可信可溯,签名验证方便高效,构建了监管系统一体化的数据身份真实可溯,为畜牧行业金融发展提供有力支持。

(2)提出的身份认证方案为聚合压缩签名算法,可有效降低签名传输通信量及系统验证开销,实现多设备接入时高效批量认证。测试分析结果表明,该方案可将签名数据通信量从线性级降低到常量级,平均验签时间节省 40.01%。同时,使用 SM2 算法对数据进行加密,保证敏感数据机密性、完整性和可用性,其密文扩散性和相关性测试结果表明密文平均改变率分别为 93.61%、93.28%,可有效保护养殖企业关键敏感数据,满足畜牧养殖资产监管过程中身份安全高效认证的需求。

参　考　文　献

[1] 国家统计局. 中国统计年鉴[J]. 北京: 中国统计出版社, 2020.

[2] 鞠光伟. 中国畜牧业保险的微观效果与政策优化研究[D]. 北京: 中国农业科学院, 2016.
JU Guangwei. Study on the micro-effect and policy optimization of China livestock insurance[D]. Beijing: Chinese Academy of Agricultural Sciences, 2016. (in Chinese)

[3] 张小栓,张梦杰,王磊,等. 畜牧养殖穿戴式信息监测技术研究现状与发展分析[J/OL]. 农业机械学报,2019,50(11):1 - 14.
ZHANG Xiaoshuan, ZHANG Mengjie, WANG Lei, et al. Research status and development analysis of wearable information monitoring technology in animal husbandry[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2019, 50(11):1 - 14. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20191101&journal_id = jcsam. DOI:10.6041/j.issn.1000-1298.2019.11.001. (in Chinese)

[4] 谢佳丽,余红,黄智良,等. 新疆农户投保肉牛养殖保险意愿的实证分析[J]. 现代畜牧兽医,2021(5):81 - 85.
XIE Jiali, YU Hong, HUANG Zhiliang, et al. An empirical analysis on farmers' willingness to insurance beef breeding in Xinjiang[J]. Modern Journal of Animal Husbandry and Veterinary Medicine, 2021(5):81 - 85. (in Chinese)

[5] SANKA A I, IRFAN M, HUANG I, et al. A survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research[J]. Computer Communications, 2021, 169: 179 - 201.

[6] 孙传恒,于华竟,徐大明,等. 农产品供应链区块链追溯技术研究进展与展望[J/OL]. 农业机械学报,2021,52(1):1 - 13.
SUN Chuanheng, YU Huajing, XU Daming, et al. Review and prospect of agri-products supply chain traceability based on blockchain technology[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(1):1 - 13. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20210101&journal_id = jcsam. DOI:10.6041/j.issn.1000-1298.2021.01.001. (in Chinese)

[7] 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018, 29(7): 2092 - 2115.
LIU Aodi, DU Xuehui, WANG Na, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092 - 2115. (in Chinese)

[8] 潍坊友容实业有限公司. 一种基于区块链的畜牧养殖管理系统:202010860978.0[P]. 2021 - 01 - 29.

[9] 唐金成,杜先培. 区块链技术驱动养殖业保险发展研究[J]. 金融理论与实践,2019(5):26 - 31.
TANG Jincheng, DU Xianpei. Research on block chain technology driving the development of aquaculture insurance[J]. Financial Theory & Practice, 2019(5):26 - 31. (in Chinese)

[10] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1 - 27.
LIU Mingda, CHEN Zuoning, SHI Yijuan, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1 - 27. (in Chinese)

[11] 何东健, 刘冬, 赵凯旋. 精准畜牧业中动物信息智能感知与行为检测研究进展[J/OL]. 农业机械学报, 2016, 47(5): 231 - 244.
HE Dongjian, LIU Dong, ZHAO Kaixuan. Review of perceiving animal information and behavior in precision livestock farming[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2016, 47(5): 231 - 244. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20160532&journal_id = jcsam. DOI: 10.6041/j.issn.1000-1298.2016.05.032. (in Chinese)

[12] 郭晓彪, 曾志, 顾力平. 电子身份认证技术应用研究[J]. 信息网络安全, 2011, 11(3): 21 - 22,25.
GUO Xiaobiao, ZENG Zhi, GU Liping. Application of electronic identity authentication technology[J]. Netinfo Security, 2011, 11(3): 21 - 22,25. (in Chinese)

[13] 耿丽微, 钱东平, 赵春辉. 基于射频技术的奶牛身份识别系统[J]. 农业工程学报, 2009, 25(5): 137 - 141.
GENG Liwei, QIAN Dongping, ZHAO Chunhui. Cow identification technology system based on radio frequency[J]. Transactions of the CSAE, 2009, 25(5): 137 - 141. (in Chinese)

[14] 张国锋, 陶莎, 于丽娜, 等. 基于植入式 RFID 感温芯片的猪体温与饮水监测系统[J/OL]. 农业机械学报, 2019, 50(增刊): 297 - 304.
ZHANG Guofeng, TAO Sha, YU Li'na, et al. Pig body temperature and drinking water monitoring system based on implantable RFID temperature chip[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2019, 50(Supp.): 297 - 304. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 2019s046&journal_id = jcsam. DOI: 10.6041/j.issn.1000-1298.2019.S0.046. (in Chinese)

[15] 许贝贝, 王文生, 郭雷风, 等. 基于非接触式的牛只身份识别研究进展与展望[J]. 中国农业科技导报, 2020, 22(7): 79 - 89.
XU Beibei, WANG Wensheng, GUO Leifeng, et al. A review and future prospects on cattle recognition based on non-contact identification[J]. Journal of Agricultural Science and Technology, 2020, 22(7): 79 - 89. (in Chinese)

[16] 赵凯旋, 何东健. 基于卷积神经网络的奶牛个体身份识别方法[J]. 农业工程学报, 2015, 31(5): 181 - 187.
ZHAO Kaixuan, HE Dongjian. Recognition of individual dairy cattle based on convolutional neural networks[J]. Transactions of the CSAE, 2015, 31(5): 181 - 187. (in Chinese)

[17] 杨毅宇,周威,赵尚儒,等.物联网安全研究综述:威胁、检测与防御[J].通信学报,2021,42(8):188 - 205.
YANG Yiyu,ZHOU Wei,ZHAO Shangru,et al. Survey of IoT security research: threats, detection and defense[J]. Journal on Communications,2021,42(8):188 - 205. (in Chinese)

[18] 左斐, 徐璋勇, 罗添元. 保险能改善对农户的信贷配给吗? ——来自 822 户农户调查的经验证据[J]. 云南财经大学学报, 2019, 35(8): 63 - 75.
ZUO Fei, XU Zhangyong, LUO Tianyuan. Can insurance improve the credit rationing of farmers? empirical evidence from the survey of 822 Chinese rural households[J]. Journal of Yunnan University of Finance and Economics, 2019, 35(8): 63 - 75. (in Chinese)

[19] 孟小峰,刘立新.基于区块链的数据透明化:问题与挑战[J].计算机研究与发展,2021,58(2):237 - 252.
MENG Xiaofeng,LIU Lixin. Blockchain-based data transparency: issues and challenges[J]. Journal of Computer Research and Development,2021,58(2):237 - 252. (in Chinese)

[20] TORKY M, HASSANEIN A E. Integrating blockchain and the internet of things in precision agriculture: analysis, opportunities, and challenges[J]. Computers and Electronics in Agriculture,2020,178:105476.

[21] LIANG Zhipeng, ZHOU Keping, GAO Rugao, et al. Special equipment safety supervision system architecture based on blockchain technology[J]. Applied Sciences,2020,10(20):7344.

[22] 杨观止, 陈鹏飞, 崔新凯, 等. NB - IoT 综述及性能测试[J]. 计算机工程, 2020, 46(1): 1 - 14.
YANG Guanzhi, CHEN Pengfei, CUI Xinkai, et al. Overview and performance test of NB - IoT[J]. Computer Engineering, 2020, 46(1): 1 - 14. (in Chinese)

[23] 田松, 李宝, 王鲲鹏. 椭圆曲线离散对数问题的研究进展[J]. 密码学报, 2015, 2(2): 177 - 188.
TIAN Song, LI Bao, WANG Kunpeng. On the progress of elliptic curve discrete logarithm problem[J]. Journal of Cryptologic Research, 2015, 2(2): 177 - 188. (in Chinese)

[24] 许芷岩, 吴黎兵, 李莉, 等. 新的无证书广义指定验证者聚合签名方案[J]. 通信学报, 2017, 38(11): 76 - 83.
XU Zhiyan, WU Libing, LI Li, et al. New certificateless aggregate signature scheme with universal designated verifier[J]. Journal on Communications, 2017, 38(11): 76 - 83. (in Chinese)

[25] MARIE S, LACHARITE. Security of BLS and BGLS signatures in a multi-user setting[J]. Cryptography & Communications Discrete Structures Boolean Functions & Sequences, 2018, 10(1): 41 - 58.