

高稳定性区块链节点存储数据防篡改仿真

李斌¹, 刘思尧², 王敏¹, 秦振威¹

(1. 国网宁夏电力有限公司 信息通信公司, 银川 750004; 2. 宁夏信通网络科技有限公司)

摘要: 与一般的区块链相比, 高稳定性区块链中的节点存储数据更容易受到防篡改威胁, 为了保证数据的安全性, 进行了高稳定性区块链节点存储数据防篡改仿真研究。通过滑动窗口分段将区块链节点存储的数据分割成多个子序列, 通过判断子序列的变化趋势给出特征函数, 利用字符串的方式表示区块链节点存储数据的时间序列组成, 基于变步长计算, 通过匹配测度的计算提取出区块链节点存储数据的关键特征。通过用户信息的加密生成用户密钥, 得到区块链节点存储数据的密文, 完成数据加密。引入水印防篡改算法, 分割嵌入数据中的水印信息, 通过水印信息与二进制信息之间的转换, 结合矩阵置乱实现区块链节点存储数据防篡改。实验结果表明, 本文方法能够有效防止区块链节点存储的数据被篡改, 保证数据的隐蔽性和安全性。

关键词: 区块链节点; 防篡改; 数据加密

中图分类号: TP302

文献标识码: A

Anti-tampering Simulation of Data Stored by High-stability Blockchain Nodes

Li Bin¹, Liu Siyao², Wang Min¹, Qin Zhenwei¹

(1. Information & Communication Company, State Grid Ningxia Electric Power Co., Ltd., Yinchuan 750004, China;

2. Ningxia Xintong Network Technology Co., Ltd.)

Abstract: Compared with the general blockchain, the data stored by the nodes in the high-stability blockchain are more vulnerable to the tamper-proof threat. In order to ensure the security of the data, a simulation study on the tamper-proof of the data stored by the nodes in the high-stability blockchain is proposed. By sliding window segmentation, the data stored by blockchain nodes are divided into multiple sub-sequences. By judging the changing trend of sub-sequences, the characteristic function is given, and the time series composition of the data stored by blockchain nodes is expressed by string. Based on the calculation of variable step size and the calculation of matching measure, the key characteristics of the data stored by blockchain nodes are extracted. Through the encryption of user information, the user's key is generated, and the ciphertext of the data stored by the blockchain node is obtained, thus completing the data encryption. The watermark tamper-proof algorithm is introduced to divide the watermark information embedded in the data. Through the conversion between watermark information and binary information, combined with the scrambling of the matrix, the tamper-proof of the data stored by blockchain nodes is realized. The experiment results show that the method in this paper can effectively prevent the data stored by blockchain nodes from being tampered with, and improve the concealment and security of data.

Keywords: blockchain nodes; tamper proof; data encryption

0 引言

近年来, 伴随区块链的兴起, 各国政府、企业以及科研院所都高度重视^[1]。如今, 区块链已经成为国家数字经济支柱产业, 并在多方面得到了广泛应用, 推动了实体经济的良性发展^[2]。但是智能化的发展使得区块链中存储信息安全成为人们关注的焦点。数据篡改是一种由非法操作引起的数据损坏现象, 导致数据中所含有的信息发生改变, 从而使其原本的价值下降甚至丢失^[3]。如何防止数据被篡改, 是目前大数据和云计算技术中的一个热点和难

题, 已引起国内外有关专家和学者的广泛关注。

李炜等人^[4]采用区块链技术解决移动机械臂操作过程中数据的防篡改和存储问题。采用一种基于多个冒名私钥对各节点进行加密操作, 利用数据聚合器将共享数据发送给数据库, 对指定的数据进行访问。使用机器人的公共密钥地址等条件构建一个独特的数据特征标识符, 使用一个存储模块对等待下载的机器人操作数据进行检测, 从而产生一个具有一定字节长度的数据特征字符串, 并对其进行加密, 确保机器人操作数据能够存储到区块链中, 从而防止机器人操作数据被篡改。仿真实验证明, 该算法在

保证系统抗篡改的同时,还可以缩短系统存储数据的时间,达到了预期的效果。杨修玮^[5]为了解决在实际的互联网环境下用户隐私数据传送安全性较差的问题,将数据挖掘技术应用到隐私数据防篡改方法中。利用数据挖掘技术对互联网上的个人信息进行了界定,并提出了一种个人信息抽取算法。通过对用户分享信息的行为进行修改和检查来应对在线个人资料分享的安全性问题。引入了一种加密方法对个人信息进行密码学分析,达到防止个人信息被盗用的目的。研究表明,在实际的互联网环境中,提出的算法能够有效提升互联网上的隐私信息安全,在更大程度上提高信息传输速度,达到综合优化的目的。

基于以上研究背景,本文提出一种区块链节点存储数据的防篡改方法,从而降低区块链中的数据出现泄露的风险。

1 区块链节点存储数据防篡改方法设计

1.1 提取区块链节点存储数据的关键特征

在高稳定性区块链中,节点存储数据是由多个时间序列 A_{it}^j 组成的, T 表示时间序列,利用滑动窗口分段的方法^[6],将区块链节点存储的数据分割成由 W 个节点构成的子序列,表示为:

$$Y_{it}^j = (A_{it}^j, \dots, A_{i(t+W-1)}^j) \quad (1)$$

式中, A_{it}^j 表示一维空间中时间序列的投影, i 表示滑动窗口的长度。

区块链节点处存储的数据会随着时间的变化而变化^[7],利用分割后的数据建立子序列的变化趋势函数,表示为:

$$\varphi_{it}^j = \sum_{m=0}^{W-2} (A_{i(t+m+1)}^j - A_{it}^j) \quad (2)$$

如果 $\varphi_{it}^j > 0$,说明子序列 Y_{it}^j 的变化趋势为逐渐上升;如果 $\varphi_{it}^j < 0$,说明子序列 Y_{it}^j 总体下降。

通过判断子序列的变化趋势,给出子序列的特征函数,即:

$$\text{shape}_{it}^j = \begin{cases} 1 & \varphi_{it}^j > 0 \\ 0 & \text{other} \end{cases} \quad (3)$$

式中的特征函数可以产生字符串“0”和字符串“1”,将两者结合在一起,用字符串的形式表示 A_{it}^j ,即:

$$FA_{it}^j = (\underbrace{0 \dots 0}_{g_1^j}, \dots, \underbrace{1 \dots 1}_{g_k^j}, \dots)^T \quad (4)$$

式中, g_1^j 表示右端点在字符串“1”中的位置。

利用字符串的方式表示区块链节点存储数据的时间序列组成^[8],实现了滑动窗口的分段,提高了关键特征提取的效率。

接着利用变步长的方法提高数据关键特征的提取速度。如果式(2)的函数值比前期小,在符号不变的情况下

就会减小步长;如果式(2)的函数值大于等于前期值,在符号不变的情况下就会增大步长。步长的判定公式如下:

$$L_{it}^j = \begin{cases} L_{i(t-1)}^j / \xi, \varphi_{it}^j \text{ 连续 } m \text{ 次同号且变小} \\ \xi L_{i(t-1)}^j, \varphi_{it}^j \text{ 连续 } m \text{ 次同号且未变小} \\ 1, \text{其他} \end{cases} \quad (5)$$

式中, ξ 表示判断步长的常数,通常大于 1, L_{it}^j 表示步长。

在保证特征提取效率和速度的基础上,通过匹配测度的计算^[9]提取出区块链节点存储数据的关键特征。

如果 $A_i^j = A_{i1}^j \dots A_{it}^j \dots A_{iT}^j$ 与 FA_i^j 在一维空间的时间序列投影具有相同的特征值,并且 q 个时间序列投影值就是 A_i 的特征向量,那么可以将 A_m 和 A_n 看作一个长度相等的 q 维时间序列,利用式(6)计算出 A_m 和 A_n 之间的匹配测度,即:

$$R(m, n) = \frac{1}{q} \sum_{j=1}^q \frac{a_j^T b_j}{a_j^T a_j + b_j^T b_j - a_j^T b_j} \quad (6)$$

式中, a_j 和 b_j 表示第 j 个指标在 q 维时间序列 A_m 和 A_n 中的特征向量。

匹配测度的计算值越大,区块链节点中存储数据的时间序列越相似,根据式(6)的计算结果,剔除相似度较低的时间序列,将相似度较高的时间序列作为区块链节点存储数据的关键特征。

1.2 加密区块链节点存储数据

将数据的关键特征保存在区块链中,当用户在客户端首次访问高稳定性区块链时,将用户的基本信息输入到区块链(加密用户名 g_i 和密码 h_j),即:

$$\alpha = R_{\text{pubs}} \{ID, t_s, R_{\text{pric}} \{h(g_i \cdot h_j), t_s, ID\}\} \quad (7)$$

式中, $R_{\text{pubs}}\{\}$ 表示基于公钥的加密处理函数, ID 表示用户访问区块链节点的地址, $R_{\text{pric}}\{\}$ 表示利用私钥加密存储数据的处理函数, t_s 表示访问的时间戳, $h(\cdot)$ 表示加密过程中的单向散列函数。

初始化处理加密后的用户信息^[10],引入一个随机数 ∂ 得到用户基本信息的明文,即:

$$M_1 = (f(ID \cdot x \cdot t_s) \cdot \partial \cdot \alpha) \quad (8)$$

式中, f 表示哈希函数, x 表示用户身份的二进制位。

将明文传输给服务器,计算出私钥 SK 和用户信息的密文,并将其传输给用户,即:

$$\begin{cases} SK = f(M_1 \cdot \alpha \cdot \beta) \\ M_2 = f(SK \cdot f(ID_i \cdot x) \cdot \partial \cdot \alpha) \end{cases} \quad (9)$$

根据式(8)和式(9)的结果判断用户信息的主属性明文 M_2 和副属性明文 M'_2 之间是否一致。若一致,则计算出用户身份的主属性明文 M_3 ;若不一致,则说明用户的身份存在风险,不允许其登录,通过区块链服务器计算出用户身份的副属性明文 M'_3 ,当 M_3 与 M'_3 一致时,用户的身份验证通过^[11],赋予用户生成转换密钥,对区块链节点

存储数据进行加密。

利用用户的密钥加密区块链节点中存储的数据,生成区块链节点存储的数据密文,表示为:

$$Z = \langle U_{k_1}(c_1), U_{k_2}(c_2), U_{k_3}(c_3) \rangle \quad (10)$$

式中, U 表示数据的加密函数, k_1 、 k_2 和 k_3 表示利用用户信息加密函数生成的密钥, c_1 、 c_2 和 c_3 表示待加密的数据。

通过对用户信息加密生成用户密钥,利用用户的密钥加密了区块链节点存储的数据。

1.3 区块链节点存储数据防篡改的实现

加密后的数据仍然存在被非法访问的风险,引入水印防篡改算法实现数据的防篡改。水印防篡改算法由水印封存和拓扑编码构成^[12],表示为:

$$E_{\text{dyn}} = \left(\begin{matrix} O_{\text{ori}}, U_{\text{key}_i}, Q_{\text{wat}}, D_{\text{map}}, D_{\text{map}}^{-1}, F_{\text{cod}}, \\ E_{\text{rec}}, W_{\text{emb}}, W_{\text{ext}}, O_{\text{emb}}, S_{\text{dat}}, S_{\text{cry}}, L_{\text{att}} \end{matrix} \right) \quad (11)$$

式中, O_{ori} 表示区块链节点的原始数据, U_{key_i} 表示用户输入的密钥, Q_{wat} 表示嵌入的水印信息, D_{map} 表示水印信息的映射函数, D_{map}^{-1} 表示 D_{map} 的逆函数, F_{cod} 表示拓扑编码函数, E_{rec} 表示识别函数, W_{emb} 表示嵌入算法, W_{ext} 表示信息提取算法, O_{emb} 表示包含水印信息的数据, S_{dat} 表示数据率, S_{cry} 表示数据的隐蔽性, L_{att} 表示区块链的抗攻击性。

水印防篡改算法是一个混沌动力学系统,在拓扑编码下算法的一维函数,表示为:

$$y_{n+1} = \frac{\zeta}{E_{\text{dyn}}} y_n (1 - y_n) \quad (12)$$

式中, ζ 表示防篡改的分支参数。

利用式(12)对嵌入数据的水印信息进行矩阵分割^[13],将数据中的水印信息转换成二进制信息。当水印信息的长度为 L^* 时,通过构造一个 $K_m \times K_n$ 的矩阵 K 给出水印信息的分支数量和单段长度,即:

$$\begin{cases} K_m = m \\ K_n = \lceil \sqrt{L^*} \rceil + 1 \end{cases} \quad (13)$$

假设 $K_m \times K_n$ 的矩阵 K 经过分段之后会产生 K_1 和 K_2 两个矩阵,通过 K 与 K_1 的异或操作得到一个全新的矩阵 W_1 ,经过转置变换之后产生矩阵 W_2 。通过矩阵 W_2 与矩阵 K_2 的异或操作产生异或矩阵 W_3 ,在转置处理下^[14],得到转置矩阵 W_4 。经过多次迭代使数据的置乱加密效果最优。

为了提高水印的数据率和数据的防篡改性能,将Info域和指针域^[15]添加到原有的区块链节点中,给出区块链节点的结构,如图1所示。

若改变 I_1 和 I_3 指针域,则不会影响数据的编码;若改变 I_2 ,则将会产生错误编码。因此,通过置乱的节点结构

可以避免区块链节点中存储的数据被恶意篡改。

2 仿真分析

2.1 搭建实验平台

为了验证文中方法对区块链节点存储数据抵抗篡改威胁的能力,进行一次仿真实验。实验平台的部署环境如下:操作系统为Windows 8、处理器频率为2.4 GHz、存储空间为64 GB、编程语言为Java语言。

在上述环境参数下搭建了防篡改实验平台,其结构如图2所示。

原始区块链节点
I_1 指针
I_2 指针
I_3 指针
Info域

图1 区块链节点结构图

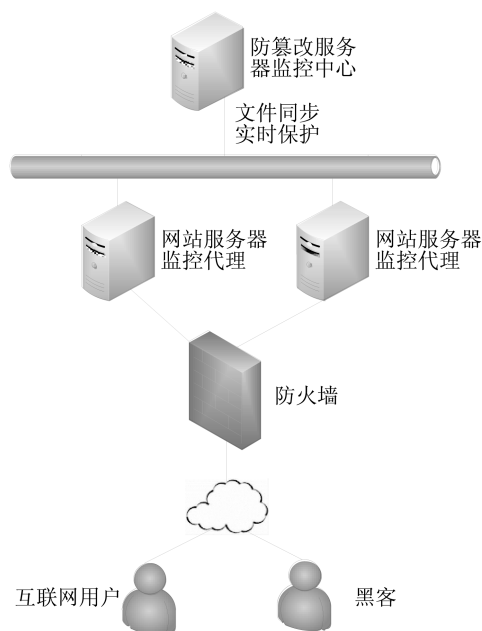


图2 实验平台结构图

在图2的实验平台中,当黑客想篡改区块链节点存储的数据时,防火墙启动,抵抗黑客的攻击。

2.2 鲁棒性验证

在实验过程中,本文选择5种数据作为测试数据,并在数据中嵌入水印信息,在不同攻击下对本文方法进行鲁棒性测试,结果如表1所列。

√表示可以恢复数据中的水印信息,×表示不可以对数据中的水印信息进行正常恢复。由表1的结果可知,采用文中方法对5种数据进行测试时,可以有效抵抗各种攻击,原因是黑客必须定位到水印信息才可以添加或者删除某一攻击,由于用户访问区块链的过程是动态的,黑客很难对区块链发起有效攻击。

表 1 对攻击的抵抗能力

攻击名称	数据 A	数据 B	数据 C	数据 D	数据 E
Inliner	✓	✓	✓	✓	✓
BLOAT	✓	✓	✓	✓	✓
Split Classes	✓	✓	✓	✓	✓
Class Splitter	✓	✓	✓	✓	✓
Array Folder	✓	✓	✓	✓	✓
Array Splitter	✓	✓	✓	✓	✓
Variable Reassigner	✓	✓	✓	✓	✓
Booleam Splitter	✓	✓	✓	✓	✓

2.3 隐蔽性分析

在隐蔽性测试中, X_{ori} 表示原始数据, X_{emb} 表示嵌入水印信息之后的数据, X_{ori} 和 X_{emb} 的相似度越高, 隐蔽性就越强。黑客很难获取到区块链节点的原始数据, 只有通过与其他数据库的对比, 才能够确定区块链节点的存储数据中是否包含水印信息, 因此, 根据 X_{ori} 与 X_{emb} 的特征, 量化处理隐蔽性指标, 计算公式为:

$$L^* = \sqrt{(a_0 - b_0)^2 + \dots + (a_n - b_n)^2} \quad (14)$$

式中, $a_0, a_1, \dots, a_n$ 表示其他数据库的指令占比; $b_0, b_1, \dots, b_n$ 表示嵌入水印信息之后区块链的指令占比。

本文搭建的实验平台能够为区块链节点提供相关的字节码函数, 因此通过编写程序得到不同指令的比率, 测试数据的隐蔽性。将本文方法量化后的隐蔽性与原始数据进行对比, 得到如图 3 所示的结果。

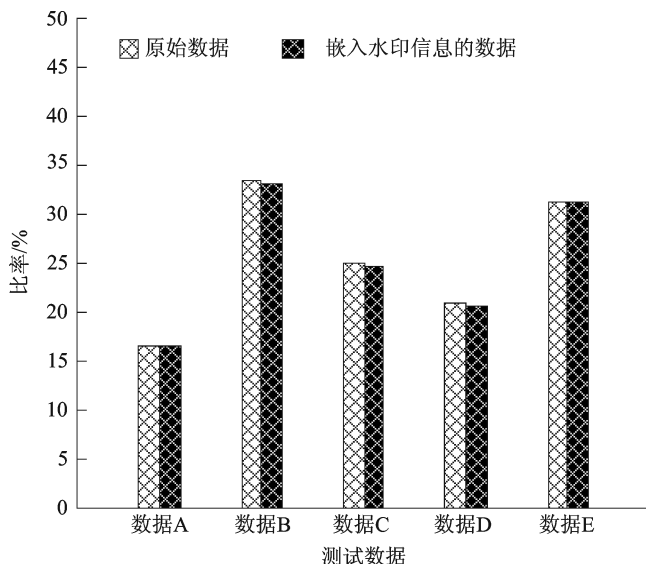


图 3 隐蔽性测试结果

由图 3 可知, 采用本文方法时, 5 种数据的隐蔽性具有较高的相似性, 嵌入水印信息的数据与原始数据之间的

比率相差在 0.015 以内, 说明采用本文方法时, 区块链节点存储数据具有较好的隐蔽性。

2.4 对比分析

为了突出本文方法的优越性, 将基于区块链技术的防篡改方法和基于数据挖掘的防篡改方法作对比, 测试了区块链节点存储数据的安全系数, 其取值范围为 0~10, 安全系数越大, 安全性就越高, 数据越不容易被篡改。图 4 给出了区块链节点存储数据的安全系数。

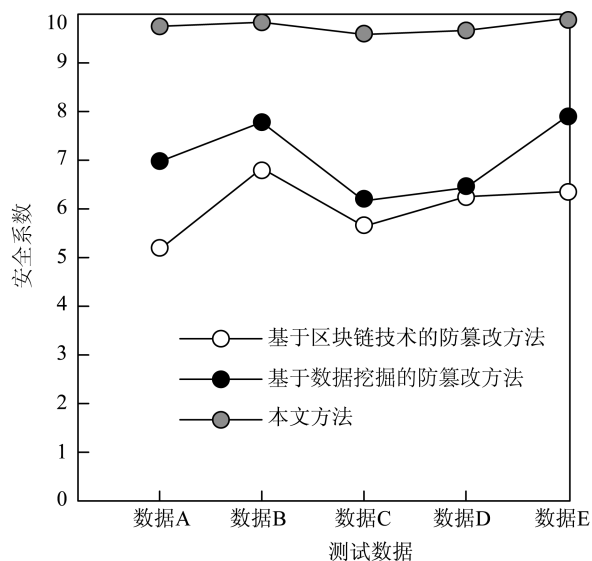


图 4 区块链节点存储数据的安全系数

图 4 中的结果显示, 与基于区块链技术的防篡改方法和基于数据挖掘的防篡改方法相比, 本文方法的区块链节点存储数据的安全系数更高(在 0.95 以上), 原因是本文方法能够根据区块链节点存储数据的关键特征对其进行加密, 防止数据被恶意篡改, 保证其安全。

3 结 语

本文提出了高稳定性区块链节点存储数据防篡改仿真研究, 经过仿真分析发现, 本文方法能够阻止黑客对区块链节点存储数据的篡改行为, 保证了数据使用的安全性。本文研究虽然取得一定成果, 但是还存在很多不足, 由于对数据的加密仅以防篡改为目的, 导致该方法对其他攻击防守的能力偏弱, 在今后的研究中, 可以设计一个由多个加密模块组成的加密系统, 从而进一步提高数据的保密性。

参考文献

- [1] 蒋宇娜, 葛晓虎, 杨旸, 等. 面向 6G 的区块链物联网数据共享和存储机制[J]. 通信学报, 2020, 41(10): 48-58.
- [2] 林霄, 姬硕, 岳胜男, 等. 面向跨数据中心网络的节点约束存储转发调度方法[J]. 计算机研究与发展, 2021, 58(2): 319-337.

- [2] YongJun Z, Cong Z, CunJun L I, et al. Fractional Fourier Transform of Ultrasonic Chirp Signal for Range Measurement[C]//The Society of Instrument and Control Engineers Annual Conference, 2015.
- [3] 关博. 基于稀疏重构及动态性分析的宽带压缩频谱感知算法研究[D]. 长春: 吉林大学, 2022.
- [4] 高磊, 宿绍莹, 陈曾平. 宽带雷达 Chirp 回波的正交稀疏表示及其在压缩感知中的应用[J]. 电子与信息学报, 2011, 33(11): 2720 - 2726.
- [5] M Arif, D M J Cowell, S Freear. Pulse Compression of Harmonic Chirp Signals Using the Fractional Fourier Transform [J]. Ultrasound in Medicine & Biology, 2010, 36(6).
- [6] 周鸿博. 基于脉冲色散处理的光子学压缩感知关键技术研究[D]. 杭州: 杭州电子科技大学, 2022.
- [7] 王硕, 郭勇, 杨立东. 分数阶傅里叶变换域的调频信号稀疏性研究[J]. 光电工程, 2020, 47(11): 40 - 47.
- [8] 齐佩汉, 李冰, 谢爱平, 等. 欠采样跳频通信信号深度学习重构方法[J]. 西安电子科技大学学报, 2022, 49(4): 1 - 7.
- [9] 宋维斌, 张圣儒, 邓忆秋, 等. 分数阶傅里叶变换域稀疏带限信号的模拟信息转换[J]. 光电工程, 2018, 45(6): 50 - 58.
- [10] 仇兆场, 陈蓉, 汪一鸣. 基于 FRFT 的线性调频信号欠采样快速检测方法[J]. 电子学报, 2012, 40(11): 2165 - 2170.
- [11] Liu B. Frequency estimation of chirp signals based on fractional fourier transform combined with Otsu's method[J]. Optik; Zeitschrift fur Licht - und Elektronenoptik; = Journal for Light and Electronoptik, 2021, 240(1).
- [12] Su H, Bao Q, Chen Z. ADMM - Net: A Deep Learning Approach for Parameter Estimation of Chirp Signals under Sub - Nyquist Sampling[J]. IEEE Access, 2020(99): 1.
- [13] 吴棋. 基于压缩传感的相移同轴分数阶傅里叶变换数字全息[J]. 信息通信, 2017(7): 17 - 21.

冯心如、银子燕(硕士研究生), 主要研究方向为信号获取与处理技术; 景宁(副教授), 主要研究方向为光通信技术。通信作者: 冯心如, 1461413004@qq.com。

(责任编辑: 薛士然 收稿日期: 2023-05-31)

- 36 [3] 吉斌, 昌力, 朱丽叶, 等. 区块链系统节点私钥泄露的电力数据防篡改方法与验证机制设计[J]. 电力自动化设备, 2021, 41(12): 87 - 94.
- [4] 李炜, 黄倩. 基于区块链技术的机器人运行数据抗篡改存储方法[J]. 科技通报, 2021, 37(11): 65 - 68.
- [5] 杨修玮. 基于数据挖掘的网络隐私数据防篡改方法研究[J]. 信息技术与信息化, 2021(12): 112 - 114.
- [6] 刘淑艳, 李丽芬. 基于信息隐藏的无线共享网络数据防篡改方法[J]. 兵器装备工程学报, 2022, 43(4): 265 - 270.
- [7] 李克楠, 邱海彬. 基于 ECC 算法的嵌入式 Linux 系统 ELF 可执行文件防篡改方法[J]. 信息技术与信息化, 2022(7): 144 - 147.
- [8] 李金讯, 郭娜, 林树鸿, 等. 基于多重图像隐藏防伪标识公文防篡改的新方法研究[J]. 电力大数据, 2021, 24(9): 1 - 8.
- [9] 张利华, 黄阳, 王欣怡, 等. 基于区块链的精准扶贫数据保护方案[J]. 应用科学学报, 2021, 39(1): 135 - 150.
- [10] 刘峰, 赵俊峰. 基于区块链的云存储数据完整性验证方案[J]. 应用科学学报, 2021, 39(1): 164 - 173.
- [11] 李晓明, 黄慧, 殷毅, 等. 基于区块链的医疗临床数据防篡改机制及篡改攻击分析[J]. 高技术通讯, 2021, 31(2): 141 - 147.
- [12] 孙传恒, 于华竟, 罗娜, 等. 基于智能合约的果蔬区块链溯源数据存储方法研究[J]. 农业机械学报, 2022, 53(8): 361 - 370.
- [13] 李姝, 赵培培, 于金刚, 等. 基于区块链的数据交易平台的研究与设计[J]. 小型微型计算机系统, 2021, 42(5): 1109 - 1114.
- [14] 许金. 煤矿安全监控系统数据防篡改研究[J]. 煤矿安全, 2020, 51(2): 116 - 119.
- [15] 方晨, 郭渊博, 王一丰, 等. 基于区块链和联邦学习的边缘计算隐私保护方法[J]. 通信学报, 2021, 42(11): 28 - 40.

李斌(高级工程师), 主要研究方向为大数据技术、人工智能技术、电力信息系统智能化运维及网络安全等; 刘思尧(高级工程师), 主要研究方向为物联网、人工智能技术、电力信息系统智能化运维及网络安全等; 王敏(工程师), 主要研究方向为大数据技术、云计算技术、数据库、智能运维技术等; 秦振威(助理工程师), 主要研究方向为信息通信信息化系统。通信作者: 李斌, nailun23258257256@163.com。

(责任编辑: 薛士然 收稿日期: 2023-05-15)

空中客车公司携手意法半导体助力飞行电动化

全球航空航天业先驱空中客车公司(Airbus, 以下简称空客)和服务多重电子应用领域、全球排名前列的半导体公司意法半导体(STMicroelectronics, 以下简称 ST)最近签署了一项功率电子技术研发合作协议, 以促进功率电子器件更高效、更轻量化, 这对于未来的混动飞机和纯电动城市飞行器发展至关重要。

在签署该合作协议前, 双方已充分评估了宽禁带半导体材料给飞机电动化带来的种种好处。与硅等传统半导体材料相比, 碳化硅(SiC)、氮化镓(GaN)等宽禁带半导体的电气性能更优异, 有助于开发更小、更轻、更高效的高性能电子器件和系统, 尤其适合那些需要高功率、高频或高温开关操作的应用领域。

该合作项目主要围绕为空客开发航空级 SiC 和 GaN 功率器件、封装和模块展开。两家公司将在电机控制单元、高低压电源转换器、无线电能传输系统等实物演示装置上进行高级研究测试, 评估功率组件的性能。