基于区块链的物流价值链数据安全共享技术*

龙 萍[1],邢 镔[2,3],胡小林[2],朱林全[2]
(1.重庆交通大学 信息科学与工程学院,重庆 400074;2.重庆工业大数据创新中心有限公司,重庆 400707;
3.工业大数据应用技术国家工程实验室,重庆 400707)

摘 要:基于工业互联网的物流供应链管理技术,业界聚焦在高精度数据分析算法的应用,对数据隐私保护算法的应用目前还处于起步阶段。然而,交易、支付环境不可信,数据易丢失及溯源难等问题,较大程度地制约了物流供应链管理技术的进一步发展。为简化过程,以物流价值链为例,将区块链技术应用于物流场景中,通过数字签名、非对称加密和 Merkle 树等算法,保障了商品数据的完整性和机密性,提供了物流订单数据溯源功能。最后,相比于业界类似技术的安全性,该方法更能满足实际工程应用对安全目标的需求,为后续落地实施提供了有力的技术支持。

关键词:供应链管理;数字签名;区块链;完整性
中图分类号:TP309.2 **文献标识码**:A **DOI**:10.19358/j.issn.2096-5133.2020.12.003
引用格式:龙萍,邢镔,胡小林,等. 基于区块链的物流价值链数据安全共享技术[J].信息技术与网络安全,2020,39(12):13-18,24.

Secure sharing technology of logistics value chain data based on blockchain

Long Ping[1], Xing Bin[2,3], Hu Xiaolin[2], Zhu Linquan[2]
(1.School of Information Science and Engineering, Chongqing Jiaotong University, Chongqing 400074, China;
2.Chongqing Innovation Center of Industrial Big-Data Co., Ltd., Chongqing 400707, China;
3.National Engineering Laboratory for Industrial Big-Data Application Technology, Chongqing 400707, China)

Abstract: Based on the industrial Internet logistics supply chain management technology, the industry focuses on the application of high-precision data analysis algorithm, the application of data privacy protection algorithm is still in the initial stage. However, problems such as unreliable transaction and payment environment, easy loss of data and difficulty in tracing the source restrict the further development of logistics supply chain management technology to a large extent. To simplify the process, we took the logistics value chain as an example and aimed to apply the blockchain technology to the logistics scene. Through algorithms such as digital signatures, asymmetric encryption and Merkle trees, our technology not only guaranteed the integrity and confidentiality of product data, but also the traceability function of logistics order data was provided. Finally, compared with the similar technologies in the industry, our method can better meet the security objectives of practical engineering applications, and provide strong technical support for subsequent implementation.
Key words: supply chain management; digital signature; blockchain; integrity

0 引言

随着工业互联网的不断发展,智慧物流作为工业 4.0 的重要发展方向,物流行业正在从传统的运营模式向集中化、信息化和智能化方向发展。尤其是在云计算、大数据和人工智能等先进技术的驱动下,智慧物流行业的服务模式得到快速发展与实践[1]。

物流供应链管理作为智慧物流的核心环节,其最终需实现进货等待耗时少、领料指引准确且高效、生产进度透明化以及监控管理便捷等目标[2-3]。将上述目标归结起来要解决的底层关键技术是如何提高数据应用的可信度。目前,业界主要聚焦在高精度数据分析算法的应用研究,对数据隐私保护算

*基金项目:国家重点研发计划(2019YFB1706100)

法的应用还处于起步阶段。

然而，可信的数据交互环境，公开、透明的物流各环节，已发生订单数据的不可篡改及物流各环节可溯源等方面，是当前物流供应链亟待解决的核心问题[4-6]。为简化描述过程，本文以制造商将产品通过物流运输送到顾客手中的过程(即物流价值链)作为示例，进行具体数据安全共享技术应用研究。

目前，针对物流价值链的数据完整性检测、安全保护及溯源三方面还存在较多不足[7]。在数据完整性检测和数据安全保护方面，当前大多数交易是基于第三方交易平台进行处理，一旦第三方交易平台发生物理损坏或遭到黑客攻击，极易使物流订单信息不准确，造成物流交付过程耗时长的问题[8]。在数据溯源方面，制造商与客户交付订单过程中，若出现商品来源、真伪以及破损等利益纠纷时，制造商很难为客户提供商品的可信来源数据和真伪凭证[9-10]。此外，若运输商品发生破损，想获取物流运输轨迹全过程的详细数据(即商品物流价值链上数据的追溯)是困难的，因此也难以进行理赔操作。

借助区块链技术的数字签名、非对称加密和共识机制等算法，实现了数据安全共享、不可篡改等特性[11]，为解决上述问题提供了重要的技术支持。文献[12]中，谢向军探讨了大数据环境下物流企业数据信息屏的安全保障体系设计要点，但未给出结合实际场景的可行应用策略。文献[13]中，严霄蕙发现了我国新零售供应链中主要面临交易、支付安全问题、物流信息与商品溯源等问题，未给出具体解决方案。文献[14]中，罗杏玲对区块链技术进行了概述，虽然提出了区块链技术在物流领域中的应用策略，但没有给出应用的具体步骤。

本文旨在将区块链技术具体地应用到物流价值链数据的安全共享环节中，并提供数据的溯源功能。为此，提出一种基于区块链的物流价值链数据安全共享技术。该技术将物流价值链数据与区块链技术深入融合，实现价值链数据的安全共享，并解决了数据处理、存储过程中的中心化和信任问题。

1 方案的架构设计与实现

区块链有助于解决当前物流业信息化、网络化、智能化发展面临的诸多难题，实现客户、制造商和物流企业三者之间的可信互联，对数据可信交换、安全共享等方面提供可靠性保护。下面将从相关技术基础和数据安全共享方案构造与实现两方面进行详细介绍。

1.1 相关技术基础

1.1.1 密码学基础

定义 1(Hash 函数) Hash 函数能够将输入任意长度的明文 M 映射为固定长度的 Hash 值：

$$H:\{0,1\}^{*}\rightarrow\{0,1\}^{k} \tag{1}$$

其中，k 表示固定序列长度。

定义 2(非对称加密算法) 非对称加密算法是利用两个不相同的密钥，分别称为公开密钥(public key，pk)和私有密钥(secret key，sk)，对应实施加密和解密操作。其中，公开密钥 pk 对明文数据 M 进行加密操作，得到密文 C：

$$C=\mathrm{Enc}_{\mathrm{pk}}(M) \tag{2}$$

在执行解密操作时，只有使用与公钥 pk 对应的私有密钥 sk 才能正确解密，得到明文 M：

$$M=\mathrm{Dec}_{\mathrm{sk}}(C)=\mathrm{Dec}_{\mathrm{sk}}(\mathrm{Enc}_{\mathrm{pk}}(M)) \tag{3}$$

由于加密和解密使用的是两个不同的密钥，因此这种算法叫做非对称加密算法[15]。具体地，非对称加密算法的加解密过程如图 1 所示。

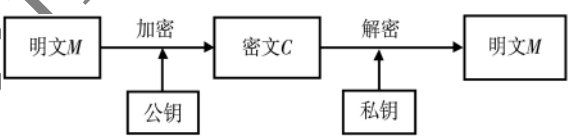

图 1 非对称加密算法示意图

定义 3(数字签名) 数字签名用于验证数据的完整性，以判断数据是否受到篡改、伪造。其中，使用私有密钥 sk 对明文数据 M 进行加密计算，得到数字签名 Sig：

$$\mathrm{Sig}=\mathrm{Enc}_{\mathrm{sk}}(M) \tag{4}$$

1.1.2 Merkle 树

Merkle 树是一种 Hash 二叉树，可以快速归纳和验证复杂有规律数据的完整性，并提供数据的追溯功能[16]。具体地，Merkle 树结构如图 2 所示。

从图 2 可以看出，Merkle 树中虚线框是由底层叶子节点(即原始物流订单数据的 Hash 值)两两组合形成一个合并 Hash 值组合，通过对其进行 Hash 计算便得到底层叶子节点对应的父亲节点。其中，$H(A,B)=H(H(A)||H(B))$。依次类推，最终可得到一棵完整 Merkle 树。

1.1.3 区块链原理

区块链是由多个有序数据区块串联而成的链式结构，且每个区块所包含的结构组成要素相同[17]。

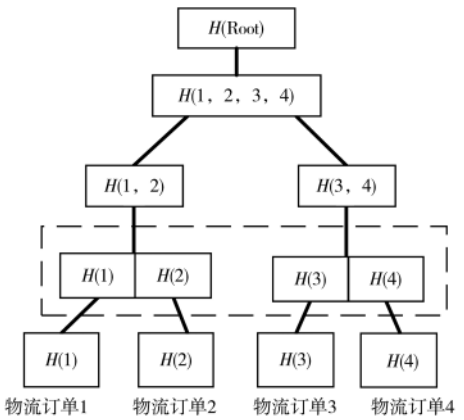

图 2 Merkle 树结构示意图

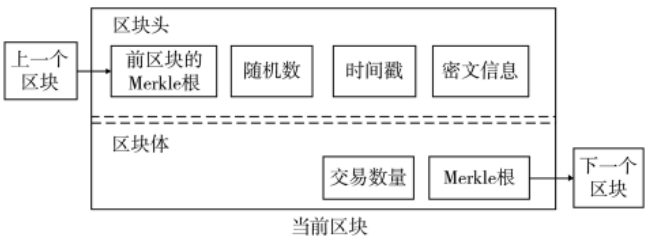

图 3 区块链结构图

大体上来说，每个区块包括区块头和区块体两部分，具体结构如图 3 所示。

其中，区块头里还封装了上一区块的 Merkle 根、随机数、时间戳以及上链存储的密文数据等信息[19]；区块体中则包含了交易数量和对应当前区块的 Merkle 根节点（将作为下一个区块头中存储的前区块 Merkle 根）[10,18]。

1.2 数据安全共享方案的设计

区块链技术是一种通过结合分布式数据存储、点对点传输、共识机制、加密算法等技术，实现数据一致存储、难以篡改、防止抵赖等功能的去中心化分布式账本技术[16]。基于区块链技术的透明化、不可篡改等特点，能够有效地解决当前物流价值链数据共享中面临的数据篡改、数据溯源难等问题，有助于实现制造商、物流企业、个人用户三方之间的数据可信互联。

具体地，订单驱动的物流数据交互示意图如图 4 所示。

物流价值链数据安全共享步骤如下：

(1)用户 A 在信息系统上提交订单，系统自动整合代表商品自身信息的原始数据 $M_{A,\text{商品}}$ 以及生成

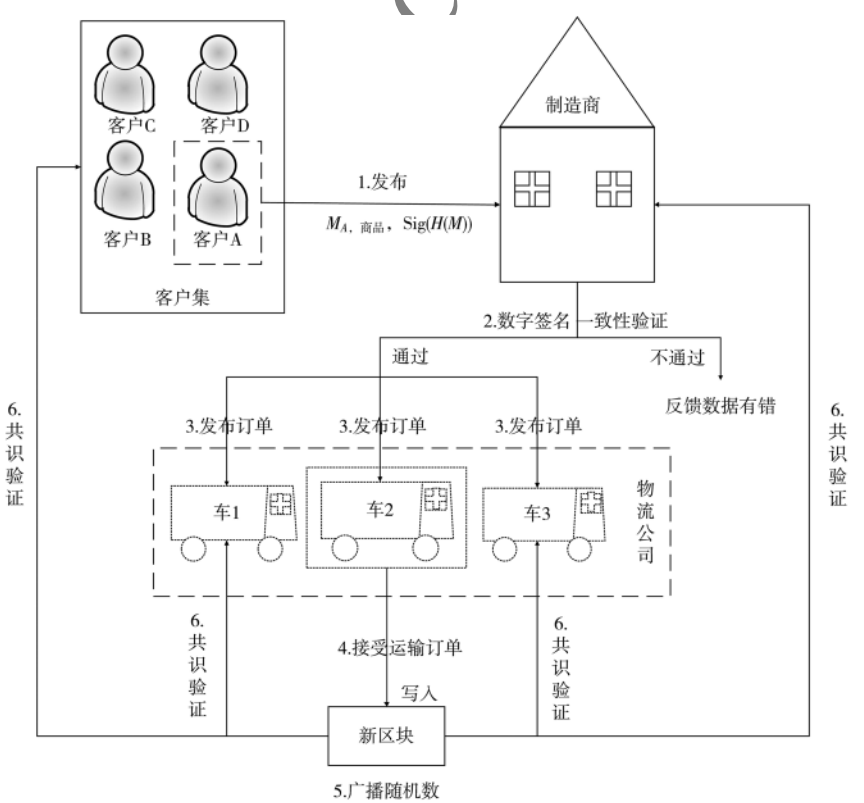

图 4 订单驱动的物流价值链数据交互示意图

公、私钥对(pk,sk)(其中(pk,sk)满足 $pk\times sk=1 \bmod q$，且 q 为一个正素数)。系统利用 Hash 函数对 $M_{A,商品}$ 进行 Hash 计算，得到 $h_{A,商品}$：

$$h_{A,商品}=H(M_{A,商品}) \tag{5}$$

接着，系统利用用户 A 的私钥 sk 对 $h_{A,商品}$ 进行加密计算，得到数字签名 $Sig_{A,商品}$：

$$Sig_{A,商品}=Enc_{sk}(h_{A,商品}) \tag{6}$$

类似地，利用用户 A 的公钥 pk 对 $M_{A,商品}$ 进行加密计算，得到密文 $C_{A,商品}$：

$$C_{A,商品}=Enc_{pk}(M_{A,商品}) \tag{7}$$

此时，将用户 A 的公、私钥(pk,sk)、商品密文数据 $C_{A,商品}$ 和数字签名 $Sig_{A,商品}$ 发送给制造商。

(2)制造商利用接收到的公钥 pk 对数字签名 $Sig_{A,订单}$ 进行解密计算：

$$h^{(1)}_{A,商品}=Dec_{pk}(Sig_{A,商品}) \tag{8}$$

$$M'_{A,商品}=Enc_{sk}(C'_{A,商品}) \tag{9}$$

接着，对式(9)计算出的商品原始数据 $M'_{A,商品}$ 进行 Hash 计算，得到 $h^{(2)}_{A,商品}$：

$$h^{(2)}_{A,商品}=H(M'_{A,商品}) \tag{10}$$

再者，制造商将计算得到的 $h^{(1)}_{A,商品}$ 和 $h^{(2)}_{A,商品}$ 的值进行一致性验证，若 $h_{-致}$ 满足：

$$h_{-致}=h^{(1)}_{A,商品}\oplus h^{(2)}_{A,商品}=0 \tag{11}$$

则该系统通过信道传输的数据是完整的。

上述步骤(2)是制造商验证数字签名的一致性，以核实传输订单数据的完整性，并生成物流订单待运输请求。若式(11)成立，则执行步骤(3)~(5)；否则，反馈数据有错误指令，终止。

(3)制造商广播物流订单数据的待运输订单数据以及商品密文数据 $C_{A,商品}$ 给合作的物流公司，由合作的物流公司进行联盟链数据资源协同，并匹配合适的物流车辆进行接单。

(4)若有物流车辆接受该待运输订单，该物流车辆将物流订单转换成其对应的 Hash 值。在收集一段时间内的物流订单数据 Hash 值后，得到所有订单数据的 Merkle 根，并将其插入新生成的区块体中。此后，再利用随机预言机采样一个随机数，将随机数、时间戳以及商品密文数据 $C_{A,商品}$ 存储在新形成的区块头中。最后，把随机数和新区块在联盟链内对所有合法节点进行广播。

(5)联盟链上的合法节点通过共识算法对接收到的随机数进行共识验证，若联盟链上的所有合法节点通过共识算法后，均达成一致结果，则将验证的新区块写入自己的区块链中。

根据步骤(5)，利用分布式共识算法向全网所有节点广播，并完成共识。为清晰描述分布式广播和共识过程，给出详细过程示意图，如图 5 所示。

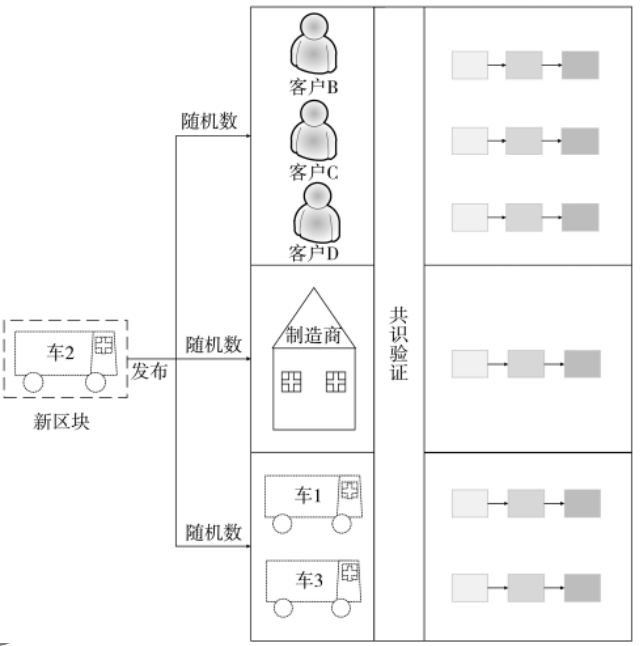

图 5 分布式共识算法示意图

新区块链接到所有合法节点主链上的许可是需要获得联盟链上所有合法节点的确认，这个过程被称作是共识机制。共识的过程：联盟链上所有合法节点利用接收到的随机数，计算其连上当前新区块 Merkle 根的哈希值，并判断计算出的哈希值前 n 位是否全为 0，若所有合法节点计算结果均满足条件，则通过共识验证，将新区块链分别接在各自的主链后。基于分布式共识算法在点对点网络的基础架构上，联盟链中各节点之间地位平等且互不影响，以快速地完成联盟链节点之间数据可信的共识验证操作。重复上述过程，即完成区块链系统的生成。

在数据共享方案的架构下，通过利用 Hash 算法、非对称加密算法、时间戳、P2P 技术及共识机制，实现了新区块的形成和协同。接下来，将对数据安全共享方案的正确性进行证明。

2 正确性证明

前一节给出了数据共享方案具体的构造与实施，本节主要针对上述方案的正确性进行证明。接

下来，将从数字签名的正确性验证和非对称加密算法的密文数据正确解密两部分进行开展。

2.1 数字签名的正确性

定理 1 订单系统将客户 A 的商品原始数据 $M_{A,商品}$ 和数字签名 $Sig_{A,商品}$ 发送给制造商 B，制造商 B 在利用用户 A 公开密钥 pk 的情况下，能够以接近 100% 的概率对数字签名进行正确的完整性验证。

证明：首先，根据用户 A 发布的商品原始数据 $M_{A,商品}$，订单生成系统会利用 Hash 函数计算其对应的 Hash 值 $h_{A,商品}=H(M_{A,商品})$。接着，订单生成系统使用用户 A 对应的私钥 sk 加密 $h_{A,商品}$，得到对应的数字签名 $Sig_{A,商品}=Enc_{sk}(h_{A,商品})$。此后，系统便将用户 A 的公钥 pk、商品原始数据 $M_{A,商品}$ 和数字签名 $Sig_{A,商品}$ 通过信道发送给制造商 B。

制造商 B 利用用户 A 发布的公钥 pk 对数字签名 $Sig_{A,商品}$ 进行解密计算，得到 $h_{A,商品}^{(1)}=Dec_{pk}(Sig_{A,商品})$ 的值。与此同时，还利用接收到的商品原始数据 $M'_{A,商品}$ 进行 Hash 计算，得到其对应的 $h_{A,商品}^{(2)}=H(M'_{A,商品})$ 值。最后，制造商 B 将计算得到的 $h_{A,商品}^{(1)}$ 和 $h_{A,商品}^{(2)}$ 的值计算 $h_{A,商品}^{(1)}\oplus h_{A,商品}^{(2)}$ 的异或值。由于只有当 $h_{A,商品}^{(1)}\oplus h_{A,商品}^{(2)}$ 的异或值等于 0 时，才能判断该数据是未被修改、完整的。此时，$h_{A,商品}^{(1)}\oplus h_{A,商品}^{(2)}=0$ 的成功概率为：

$$\Pr[h_{A,商品}^{(1)}\oplus h_{A,商品}^{(2)}=0]=1-\frac{1}{2^{256}}\approx 1 \tag{12}$$

若商品原始数据 $M_{A,商品}$ 和数字签名 $Sig_{A,商品}$ 中至少有一方数据是丢失（不完整或者被篡改）、伪造的，则不能通过数据的完整性检测。具体地，数字签名正确性验证示意图如图 6 所示。

2.2 非对称加密算法的数据正确解密

定理 2 用户 A 在使用私有密钥 sk 的情况下，能够对密文数据 C 实现正确解密。

证明：根据非对称加密算法需要产生公开密钥 pk 和私有密钥 sk 两个不同的密钥，其中，密文 $C_{A,商品}=Enc_{pk}(M_{A,商品})$ 是通过使用公开密钥 pk 对商品数据 M 加密得到的。公、私钥对 (pk，sk) 满足 $pk\times sk=1 \bmod q$，且 q 为一个正素数。因此，使用私有密钥 sk 对密文 C 进行解密计算，得到：

$$\begin{aligned}Dec_{sk}(C_{A,商品})&=Dec_{sk}(Enc_{pk}(M_{A,商品}))\\&=(Dec_{sk}Enc_{pk}(M_{A,商品}))\\&=(Dec_{sk}Dec^{-1}{}_{sk}(M_{A,商品}))\\&=M_{A,商品}\end{aligned} \tag{13}$$

证毕。

3 安全性分析

上一节给出了本文方案的正确性证明，本节将对所提方案的安全性进行分析。接下来，从 Hash 函数、数字签名以及时间戳机制 3 方面对方案的安全性进行全面分析。

3.1 Hash 函数的不可逆性

Hash 函数可以将任意输入长度的数据通过压缩计算后，使用 Hash 值来替代表示。因此，区块链上存储的数据不是现实世界的交易数据，而是原始数据对应的 Hash 值，并通过哈希二叉树结构，将其简化为 Merkle 根记录到区块链中。另外，Hash 函数还存在以下优点[18]：

(1) 不可逆性：仅知道 Hash 值不能得出与其对应的明文数据 M_1；

(2) 抗弱碰撞性：找到与给定明文数据 M_1 具有相同 Hash 值的另一个明文数据 M_2 的概率是可忽

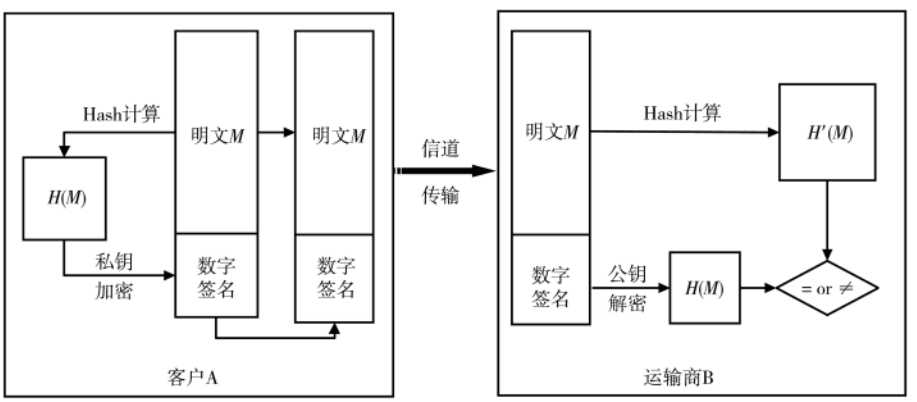

图 6 数字签名正确性验证示意图

略的；

(3)抗强碰撞性：给定明文数据 M_1 和 M_2，它们具有相同 Hash 值的概率是可忽略的。

根据上述 3 个特点，Hash 函数能够保障存储在区块链中的商品原始数据的机密性和安全性。

3.2 数字签名的安全性

定理 3 非法用户在没有合法私钥 sk 的情况下，伪造正确数字签名的成功概率：

$$\Pr[\mathrm{Sig}_{sk}(H(M))=\mathrm{Sig}_{sk'}(H(M))|\text{猜测 sk}']=\frac{1}{2^{256}}\approx 0 \tag{14}$$

该概率是可忽略的。

证明：根据非对称加密算法，已知公钥 pk，破解私钥 sk 的困难性是可以归约大整数分解的 NP 困难问题，即在多项式时间内是难解的。因此，定理 3 的结论显然成立。

3.3 时间机制的单向性

定理 4 时间具有单向性，因此在已加盖时间戳的文件数据上，非法用户无法伪造对应的文件数据。

以上是显然成立的。

4 性能分析

本方案通过将区块链技术应用于物流场景中，通过数字签名、非对称加密和 Merkle 树等算法，保障商品数据的完整性和机密性，提供物流订单数据溯源功能，最终实现物流价值链数据的安全共享。其中，本方案使用的数字签名和非对称算法，在加、解密过程的时间复杂度分析结果如表 1 所示。

表 1 数字签名和非对称算法的时间复杂度分析结果

过程	数字签名	非对称算法
加密	$O(k)$	$O(k)$
解密	$O(k)$	$O(k)$

表 1 中，数字签名和非对称算法在加密、解密过程的时间花销均为线性时间复杂度 $O(k)$，在实际应用场景中具有可行性。

此外，本方案相较于业界成熟物流价值链数据管理应用，有以下 3 点优势：

(1)基于数字签名技术的特性，能够确保上链商品数据的完整性，提升数据的可信度，有利于缩短物流环节总耗时；

(2)基于非对称加密算法、分布式存储以及共识机制的特征，能够给联盟链上的参与节点提供公平可信的交易、支付环境，实现联盟链上物流订单数据的安全共享，使物流订单数据实现高效、可信协同；

(3)在通过共识机制的验证后，合法节点会在各自主链末端链接上新区块，方便各节点根据区块体中所包含的 Merkle 根，对商品物流订单信息进行溯源追踪。

5 结论

本文所提出的数据安全共享技术，解决了交易、支付环境不可信，物流数据容易丢失、篡改以及商品物流订单溯源难等问题，为物流价值链数据安全共享环节中的区块链技术应用，提供了有力的技术支持和实施步骤指导。

未来，本文所提技术可从工业应用与理论改进两个角度着手实施进一步的研究。一方面，可将本技术封装为工业微服务，应用于可信工业互联网平台建设，实现用户安全需求与工业应用技术的高效融合。另一方面，随着未来量子计算等新科技的发展，区块链技术中基于确定性的非对称加密算法有可能存在被破解的风险，因此，基于同态加密技术融合的抗量子非对称加密算法，可以考虑融入到区块链技术中，以抵抗量子计算攻击。

参考文献

[1] 王献美.基于大数据的智慧云物流理论、方法及其应用研究[D].杭州：浙江理工大学，2018.

[2] 陈勇，于斌，许梦恬，等.智能制造背景下的智慧物流供应链建设研究[J].现代商业，2019(14)：7-8.

[3] 陈雁云.企业物流供应链管理[J].现代企业文化，2012(32)：61-62.

[4] 陈利，袁蓉，刘永刚.基于物联网的智能物流供应链管理研究[J].商品与质量，2011(S5)：238-239.

[5] 张颖川，赵皎云.共筑智能制造与智慧物流新生态——2019 第四届全球制造业供应链与物流技术研讨会侧记[J].物流技术与应用，2019，24(6)：70-78.

[6] 李嘉诚.大数据环境下物流企业的数据信息安全保障策略[J].物流工程与管理，2016，38(4)：168-169.

[7] 陈涛，马敏，徐晓林.区块链在智慧城市信息共享与使用中的应用研究[J].电子政务，2018(7)：28-37.

[8] CHRISTIDIS K，DEVETSIKIOTIS M.Blockchains and smart contracts for the Internet of Things[J].IEEE Access，2016(4)：2292-2303.

(下转第 24 页)

下误区：一是工业尤其是工控系统信息相对安全，缺乏推进工作的主动性；二是认为隔离的工业网络就绝对安全，其内部网络、主机和设备基本不作安全防范，一旦网络隔离被突破将造成严重影响；三是工业主机、工控系统等的操作系统、软件应用版本老旧，且认为进行补丁升级操作将带来生产安全风险或无法得到生产厂商维保服务，而几乎不作补丁升级，存在安全隐患；四是认为部署持续性的在线安全监测手段不必要，使得应对突发性的漏洞、病毒等事件不及时，应急措施严重缺乏。

建议企业注重发展过程中的信息安全风险，按照《中华人民共和国网络安全法》要求，落实网络安全主体责任和等级保护等基本安全制度；对照《工业控制系统信息安全防护指南》等的有关要求，对工业互联网中的安全薄弱环节，重点加强工业网络、主机、控制设备的安全软件部署和安全配置，软件补丁升级管理，生产网、办公网等网络隔离，互联网远程访问控制，以及外连设备安全连入管理等有关工作。

参考文献

[1] GB/T 22080-2016/ISO/IEC27001：2013 信息技术 安全技术 信息安全管理体系 要求[S].2016.

[2] ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT[EB/OL].[2020-09-01].https://www.iso.org/isoiec-27001-information-security.html.

[3] GB/T 29246-2017/ISO/IEC 27000：2016 信息技术 安全技术 信息安全管理体系 概述和词汇[S].2017.

[4] GB/T 20984-2007 信息安全技术 信息安全风险评估规范[S].2007.

[5] 邢栩嘉，林闯，蒋屹新.计算机系统脆弱性评估研究[J].计算机学报，2004(1)：1-11.

[6] Common Vulnerability and Exposures[EB/OL].[2020-09-01].http://cve.mitre.org/.

[7] GB/T 22081-2016/ISO/IEC27002:2013 信息技术 安全技术 信息安全控制实践指南[S].2016.

[8] 韦正现，宋敏，童鹏鹏，等.一种基于信息熵的体系流程脆弱性分析方法[J].科技导报，2019，37(13)：40-46.

(收稿日期：2020-09-28)

作者简介：

魏为民(1970-)，男，博士，副教授，主要研究方向：信息安全、图像处理、数字取证和信息隐藏。

张运琴(1996-)，男，硕士研究生，主要研究方向：信息安全、图像处理。

翟亚红(1974-)，女，本科，高级工程师，主要研究方向：网络安全与认证认可。

(上接第 18 页)

[9] 顾欣，徐淑珍.区块链技术的安全问题研究综述[J].信息安全研究，2018，4(11)：997-1001.

[10] 王静，蒋国平.一种超混沌图像加密算法的安全性分析及其改进[J].物理学报，2011(6)：89-99.

[11] 呼阳，陈亮.基于区块链的生产线数据共享方案研究[J].国外电子测量技术，2019(5)：123-127.

[12] 谢向军.大数据环境下物流企业的数据信息安全保障对策分析[J].信息通信，2017(6)：34-36.

[13] 严霄蕙.区块链技术驱动下的新零售业态变化与发展路径[J].技术经济与管理研究，2019，27(1)：13-18.

[14] 罗杏玲.区块链技术在物流领域中的应用探索[J].中国商论，2017(24)：7-8.

[15] 彭长根，田有亮，刘海，等.密码学与博弈论的交叉研究综述[J].密码学报，2017，4(1)：1-15.

[16] 吴腾，黄锴，周琳琳，等.具有状态合法性验证的区块链一致性算法研究[J].计算机工程，2018，44(1)：160-164.

[17] GERVAIS A，KARAME G O，WÜST K，et al.On the security and performance of proof of work blockchains[C].ACM Sigsac Conference on Computer & Communications Security.ACM，2016.

[18] PASS R，SEEMAN L，SHELAT A.Analysis of the blockchain protocol in asynchronous networks[C].Annual International Conference on the Theory and Applications of Cryptographic Techniques.Paris，France，2017.

(收稿日期：2020-09-09)

作者简介：

龙萍(1995-)，女，硕士研究生，主要研究方向：区块链、数据安全与隐私保护。

邢镔(1962-)，通信作者，男，博士，教授级高级工程师，主要研究方向：智能制造、数据处理和工业数字仿真。E-mail：xingbin@casic.com.cn。

胡小林(1984-)，男，硕士，研究员，主要研究方向：智慧物流、智能仓储。

版权声明