·体系结构与软件技术· 文章编号：1000-3428(2018)12-0085-09 文献标志码：A 中图分类号：TP391

基于比特币技术的供应链管控与溯源方案

陆 尧，文 捷

（复旦大学 计算机科学与技术学院 复旦-众安区块链与信息安全联合实验室，上海 200433）

摘 要：供应链管控系统多数采用中心化设计，系统负载上限受制于中心服务器性能，导致整条供应链无法正常流动。为此，提出一种结合区块链、比特币协议确定性分层钱包与多重签名技术的方案，以满足供应链中产品编码、权限管理、物权转移、产品溯源和防伪验证等需求。将供应链内部实体分为“人物实体”“产品实体”和“权限实体”，利用分层钱包技术进行实体密钥的分配。给出基于分层钱包技术的树形结构编码体系，并设计基于区块链交易的去中心化权限管控、物权转移信息记录与验证机制。分析结果表明，该方案具有区块链去中心化、交易可回溯和不可篡改等特性，可解决现有技术中的常见的问题，相比传统供应链管控方案有较大的优势。

关键词：供应链管控；区块链；比特币；分层钱包；多重签名；产品溯源

中文引用格式：陆 尧，文 捷. 基于比特币技术的供应链管控与溯源方案[J]. 计算机工程，2018，44(12)：85-93，101.

英文引用格式：LU Yao，WEN Jie. Scheme of supply chain control and traceability based on Bitcoin technology[J]. Computer Engineering，2018，44(12)：85-93，101.

Scheme of Supply Chain Control and Traceability Based on Bitcoin Technology

LU Yao，WEN Jie

（Fudan-Zhong'an Block Chain and Information Security Joint Lab，School of Computer Science and Technology，Fudan University，Shanghai 200433，China）

【Abstract】Most of the supply chain control systems adopt a centralized design，and the system load ceiling is severely constrained by the performance of the central server，resulting in the entire supply chain not flowing properly. Therefore，a scheme combining blockchain，Bitcoin protocol deterministic layered wallet and multi-signature technology is proposed to meet the requirements of product coding，rights management，property transfer，product traceability and anti-counterfeiting verification in the supply chain. The internal entities of the supply chain are divided into " personal entities" " product entities" and " right entities" ，and the entity key is allocated by using the layered wallet technology. The tree structure coding system based on layered wallet technology is given，and the mechanism of decentralized right management and property transfer information recording and verification based on blockchain transaction is designed. Analysis results show that the scheme has the characteristics of blockchain decentralization，transaction traceability and non-tamperability，which can solve common problems in existing technologies and systems，and has greater advantages compared with traditional supply chain control schemes.

【Key words】supply chain control；blockchain；Bitcoin；hierarchical wallet；multi-signature；product traceability

DOI：10.19678/j.issn.1000-3428.0048505

0 概述

供应链的通用定义为“在产品生产和流通过程中，一个由供应商、制造商、分销商、零售商和最终消费者等组成的自上而下的连接网络”[1]，供应链管控是现代企业市场竞争力的重要组成部分。由于供应链在流动中涉及到大量的数据处理和交互，将互联网技术引入供应链管控，实现供应链全程信息化已成为一种趋势。利用管理学、金融学、统计学和计算机科学等各学科的最新成果，提升供应链的效率和安全性是当今业界研究的热点之一。

本文总结供应链管控中的几个关键因素，基于相关领域现有的研究与应用，结合区块链、分层钱包和多重签名技术，提出一种新型的供应链管控与溯源方案。该方案利用比特币及区块链技术在去中心化、可溯源、防篡改、信息安全等方面的优势，可为区

基金项目：国家自然科学基金(61672166)；2016 年上海市领军人才计划项目(021)；2016 年上海市优秀学术带头人人才计划项目(16XD1400200)；上海市基础研究科技创新行动计划项目(16JC1402700)。

作者简介：陆 尧(1992—)，男，硕士研究生，主研方向为信息安全、区块链；文 捷，工程师。

收稿日期：2017-09-01 **修回日期：**2017-11-09 **E-mail：**15210240013@fudan.edu.cn

块链技术的推广与应用提供一种新的思路。

1 研究现状

现阶段,供应链管控及其信息化是学术界和工业界共同的研究热点。如:文献[2]论述了目前供应链管控的关键因素、常用策略和设计方向;文献[3]总结分析了供应链管控中各类建模方法的特点和优劣;文献[4]提出了评判供应链性能的几个关键指标和测量框架;文献[5]提出一种基于 SCOR 模型的信息化供应链管控方案,使计算机可以辅助和监控供应链的流动;文献[6]设计实现了一个基于 RFID 与物联网技术的供应链信息交互模型,提升了供应链在信息获取、数据流通和整体监控上的效率。在工业界中,沃尔玛利用条形码(UPC)技术和射频数据通信(RFDC)技术构建了一条低成本、高效率的补货系统,大幅提升了毛利率[7];京东在 2016 年完成了全供应链的电子化改造,数据显示仅在仓储交接阶段,每年就为其节省了约一亿元开销[8]。

现有的信息化供应链管控研究成果与应用方案,主要存在如下的可改进环节:

1)大部分供应链管控系统采用中心化设计,系统负载上限严重受制于中心服务器性能。一旦企业业务需求快速扩张,原有系统极可能不堪重负,导致整条供应链无法正常流动;并且中心化系统的软硬件升级不仅非常困难,而且成本极高。以 IBM 服务器为例,由一套中等配置的小型机升级至大型机解决方案需要上亿元的投入。

2)现阶段所有管控系统都使用数据库记录供应链信息。在数据库的选择上,若使用中心式数据库,则会导致中心服务器性能瓶颈和中心服务器强依赖性等问题;若使用分布式数据库,则会产生系统通信开销大、存取结构复杂、安全性降低和难于维护等问题[9]。

3)管控系统的安全性完全依赖于中心服务器和数据库。一旦两者被攻破,所有用户信息、交易记录和其他关键数据将全部暴露甚至被篡改,给供应链的所有参与者带来严重安全威胁。

4)在实际商业应用中,产品的防伪验证是具有重要需求。现有方案大多采用“验证码 + 验证平台”的形式,需要用户连接厂家验证平台后验证防伪信息。在该方式中,不仅验证码极易被伪造与冒用,维护一个庞大的验证平台也需要非常大的开销。

针对上述问题,本文结合区块链、分层钱包和多重签名技术,设计了一种基于比特币技术的供应链管控方案。本文的主要贡献如下:

1)将现在仅存于比特币和以太坊系统中的确定性分层钱包技术引入到权限管控领域中,在编码上直接表达权限的区分和层级关系。这种方案可以推广至物联网编码领域,构建一套层级关系明确、空间充足的编码体系。

2)利用区块链记录系统正常运行所需的信息,数据库系统仅作为辅助工具使用。方案在运行上采用半中心化的架构,系统的所有者拥有较高的控制权。区块链在生产环境下中心化与去中心化的优劣之争不断,本文方案提供了一种相对平衡的解决方式。

3)扩展了区块链交易的应用场景。现阶段基于区块链的各类应用大多采用改变区块链交易中记录内容的方式,以满足不同的需求。本文方案直接使用区块链交易本身来表达信息,是一种区块链应用上的创新,为区块链技术的推广和应用提出了新的思路。

4)充分利用区块链和比特币技术中在去中心化、信息可溯源与不可篡改等方面上的特性,设计了一套完整的信息化供应链管控方案,解决了现有系统存在的一些问题。

2 方案背景技术

2.1 区块链

区块链作为比特币的底层技术,承载着验证并记录合法比特币交易的功能[10]。“区块”是一个聚合了部分交易信息的容器类数据结构,一般由一个包含元数据的区块头和紧随其后的一系列交易组成。对每个区块头进行 SHA256 运算后[11],可以得到一个用于标识该区块的哈希值。区块链是由区块构成的一种有序链型数据结构,链中每个区块都包含前区块的哈希值,可以由链上任意区块追溯到第一个区块(创始块),其结构如图 1 所示。

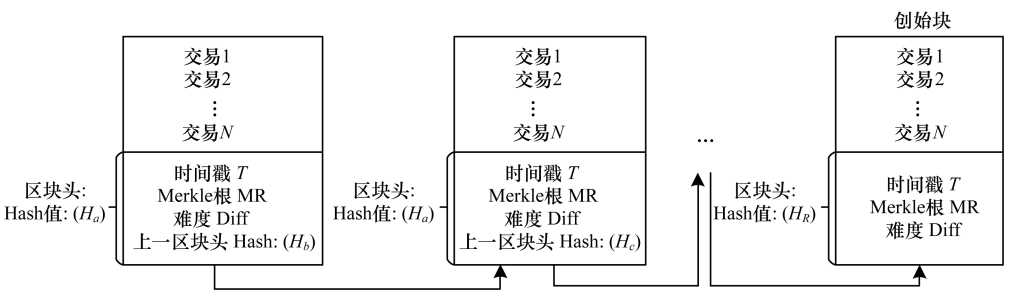

图 1 区块链结构

由于区块头包含了父区块的哈希值,因此当前区块的哈希值会受到父区块的影响。一旦某区块发生改变,所有后续区块必须全部重新计算。当一个区块拥有了足够多的后续区块后,对它的任何改动将消耗难以承受的巨大算力,所以一条足够长的区块链可以保证其记录的信息不可更改,这是区块链安全性的重要基础。

2.2　非对称加密与比特币密钥

非对称加密算法是信息安全领域的数学基础之一。在非对称加密算法中,密钥由一对数学相关的公钥和私钥组成,公钥完全公开,可在不安全的条件下传输和储存,私钥则必须保密。在算法中,若公钥为加密密钥,则发送方可在任意网络上发送加密信息,只有私钥的拥有者可以正确解密,即实现了数据的加密传输。若公钥为解密密钥,则只有通过私钥加密的信息(也即数字签名),才可以被该公钥正确地解密,即实现了数据的来源验证。

比特币系统使用非对称加密算法来控制比特币的所有权。比特币密钥是一对"私钥/公钥"对,公钥为解密密钥。当一笔新的支付交易进入网络后,网络节点会利用支付者的公钥验证交易中数字签名的合法性,从而确定交易是否来源与比特币的所有者。

2.3　确定性分层钱包

"比特币钱包"指用于存储密钥的加密存储文件或数据库,用户可以在钱包中生成多对密钥。钱包总体上分为 2 类:非确定性(随机)钱包和确定性(种子)钱包。

非确定性钱包随机生成部分相互无关的私钥。由于私钥之间没有关联,因此需要备份钱包中所有的密钥。一旦某个密钥丢失,它控制的所有比特币也会丢失。因此,非确定性钱包难于管理和备份。

为了改进上述问题,比特币 BIP0032 标准中提出了"分层确定性钱包"(Hierarchical Deterministic Wallet, HDW)技术。分层钱包生成一个128 bit到256 bit 的随机数作为"种子",钱包中所有的密钥都衍生自这个种子及其哈希后的"链码"。并且,每对密钥同样可以通过哈希获得自己的"链码"以衍生下一层密钥。最终,分层钱包的所有密钥构成一个具有层级关系的树状结构。

分层钱包的优势主要有 3 个:1)只要备份种子就能还原整个密钥树;2)树状结构在应用中可以表达额外的组织含义,例如某个分支用作收入,另一个用作消费;3)在分层钱包中子公钥可由父公钥直接衍生,这就允许在不接触私钥的情况下,衍生出一系列合法的公钥。

2.4　多重签名

数字签名是非对称密码系统的一个重要的应用,用于确认信息来源。消息发送方使用哈希函数从信息中提取一段摘要并用私钥加密(签名),接收方利用公钥解密签名,若其与采用相同哈希函数提取的摘要相同,则能确认消息来自密钥的所有者。

在比特币和其他区块链系统中,签名算法用于保证交易的合法性。区块中每条交易记录都有一个混合了交易信息和接收方密钥的锁定脚本。当接收方发起一个新的交易时,必须提供上一个交易输出中锁定脚本对应的公钥和数字签名(解锁),才能被系统接纳并记录到账本(区块链)中。以此为基础,整个比特币网络在不需要中心机构的情况下,实现了交易的自动验证和比特币所有权的安全转移。

在实际应用中,出于安全和管理等原因,一些比特币交易需要经由不同的实体同时许可才能完成。比特币协议采用多重签名技术实现该需求,多重签名交易的锁定脚本记录了 N 个公钥及其对应签名,至少需要提供其中的 $M(M \leqslant N)$ 个才可以解锁交易输出,从而发起新的交易。

3　方案设计

3.1　方案整体架构与流程

本文方案整体架构如图 2 所示。

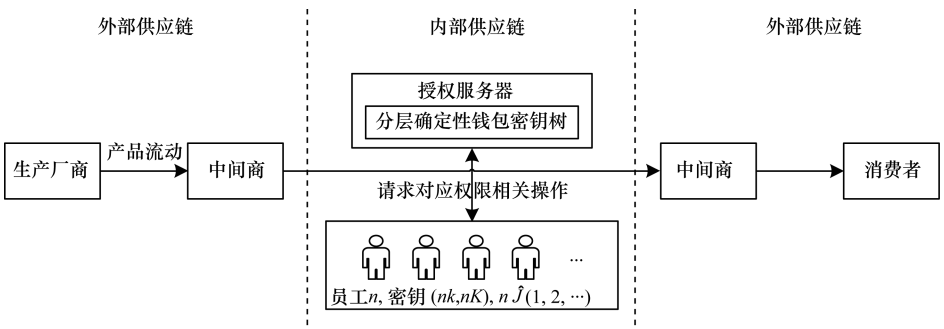

图 2　本文方案整体架构

一般而言,供应链可分为内部与外部两类。内部供应链指企业内部产品在生产和流通过程中涉及的采购、制造、分销、仓储等部门构成的供需网络;外部供应链指企业外部参与企业相关产品生产与流通的原材料供应商、生产厂商、储运商、零售商和最终消费者组成的供需网络[12]。本文方案针对外部和

内部供应链采用了不同的架构。

在外部供应链上,方案使用去中心化设计。上游生产商、中游储运与零售商和下游的消费者之间没有逻辑关系,密钥相互独立;在内部供应链上,方案使用“验证授权”的方式,维护一个保存分层密钥的授权服务器 。内部员工仍保有自己的密钥,但进行操作时,需要向授权服务器请求自己级别的密钥。内部的私钥不对外公开。

本文方案并不限制底层的区块链平台。无论使用以太网、Fabric 或其他类似的区块链平台,只要提供基本的查询、交易和部署链码等功能即可。

3.2 密钥分配

在本文方案中,每个实体都拥有一对密钥。本文将密钥表示为(xk,xK),其中,xk 为私钥,xK 为公钥,x 为密钥的持有实体,$(xk,xK)\Rightarrow(yk,yK)$表示在分层钱包中,父密钥$(xk,xK)$衍生出子密钥$(yk,yK)$,或$(yk,yK)$是由父密钥$(xk,xK)$衍生出的子密钥。

本文方案的密钥分配可分为 3 类:人物实体,产品实体和权限实体。

1)人物实体密钥分配

本文方案人物实体(例如供应商的物流员工,终端消费者等)的密钥(xk,xK)唯一且相互无关联。在采用安全随机源的情况下,该条件很容易达到。

2)产品实体密钥分配

产品实体指供应链源头处的相关实体,包含生产商、代工厂、生产商的所有产品及其对应的物理单品。产品实体的密钥在生产阶段采用分层钱包技术分配。

假设产品生产商为 P,拥有一对主密钥(Pk,PK)。$P_i\in P,i\in\{1,2,\cdots\}$表示 P_i 是 P 的一个代工厂。$p\in P$ 表示 p 是 P 生产的一款产品。$p_j\in P_i,j\in\{1,2,\cdots\}$表示 p_j 为 p 的一件单品,该单品由代工厂 p_i 生产。

产品实体的密钥分配方式如下:

$$(Pk,PK)\Rightarrow(P_ik,P_iK),i\in\{1,2,\cdots\}$$

$$(Pk,PK)\Rightarrow(pk,pK)$$

$$(pk,pK)\Rightarrow(p_jk,p_jK),j\in\{1,2,\cdots\}$$

其中,p_jK 可以作为单品 p_j 的唯一标识。该标识空间约为 2^{32}个,完全满足生产需要。

3)权限实体密钥分配

权限实体指在内部供应链中,授权服务器 Serv 内部保存的权限,例如公司中“董事长”“总经理”或“物流员工”等职位。权限实体的密钥在授权服务器 Serv 内部采用分层钱包技术分配。

假设使用内部供应链的机构为 T,拥有一对主密钥(Tk,TK)。权限可以表达为一个树状结构,父节点拥有更高的权限,对自己的子孙节点持有管控权。

权限实体的密钥分配方式为:

$$(Hk,HK)\Rightarrow(L_ik,L_iK),i\in\{1,2,\cdots\}$$

其中,H 为高级权限,L_i 为 H 管控的下一级权限,表示为 $H\supset L_i$。

为避免最高权限数量不唯一,主密钥(Tk,TK)不直接代表最高权限,而是将(Tk,TK)衍生出的第一代子密钥作为最高权限实体的密钥。

授权服务器 Serv 内部的权限实体密钥结构如图 3所示。

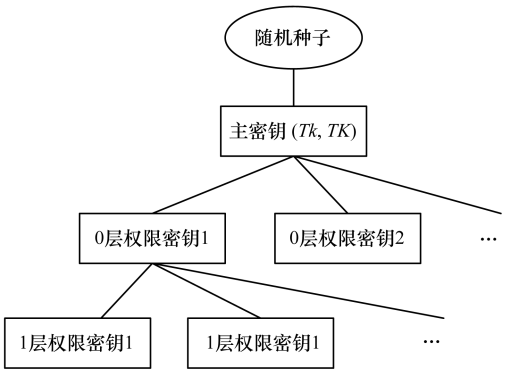

图 3 授权服务器 Serv 内部密钥结构

3.3 权限管控

权限管控分为“授权”“除权”和“查询权限”3 个部分。本文方案将权限管控的相关信息全部以交易的形式置于区块链上,交易的形式化表示如下:

$$Sig_{in1}\&Sig_{in2}\&\cdots\rightarrow Sig_{out1}\&Sig_{out2}\&\cdots$$

其中,Sig_{in}表示该交易的“输入签名”,记录了交易来源,多个输入说明来源为一个“多重签名”,即该交易由多方确认达成,Sig_{out}表示该交易的“输出解锁条件”,记录了以该交易为输入,创建新交易需要的(多重)签名。

3.3.1 授权

授权阶段需要授权服务器 Serv、授权人 $a\in X$ 和被授权人 b 三方参与。a 授予 b 的权限 Y 必须低于 a 的权限 X,且为 X 的直接下属,表示为 $Y\subset X$。

授权操作需要 3 个交易来表达,流程如下:

```
//a 向 Serv 发送授权请求 b∈Y
a request Serv with b∈Y
//Serv 验证 a 身份和权限
if a∈Y and Y⊂X
//创建交易 1,发出授权信息
create transaction None→Sig_a & Sig_X
//创建交易 2,确认被授权人
if verify (Sig_a) and verify (Sig_X)
create transaction Sig_a & Sig_X→Sig_b & Sig_Y
//创建交易 3,被授权人接受授权
if verify (Sig_b) create transaction Sig_b & Sig_Y→Sig_Y
```

交易 1 没有输入签名,类似与比特币系统中的“创币交易”。

由于 X 的私钥 Xk 仅保存在 Serv 内部,交易 1 和交易 2 需要 Serv 辅助完成(生成 Sig_X)。3 个交易

完整地记录了授权人 a 及其权限 X、被授权人 b、被授予的权限 Y 和授权时间等信息,且授权流程需要双方共同确认(使用私钥签名交易)完成。

3.3.2　除权

除权阶段需要授权服务器 Serv、除权人 $c \in Z$ 两方参与。其中,c 的权限 Z 必须高于需要解除的权限 Y,且为 Y 的直接上属,表达为 $Z \supset Y$。

除权操作需要 2 个区块链交易来表达,流程如下:

```
//c 向 Serv 发送除权请求 b ∉ Y
c request Serv with b ∉ Y
//Serv 验证 c 身份和权限
if c ∈ Z and Z ⊃ Y
//创建交易 4,发出除权信息,确认除权人
create transaction Sig_Y→Sig_c & Sig_Z
//创建交易 5,除权人确认除权
if verify (Sig_c) and verify (Sig_Z)
create transaction Sig_c & Sig_Z→Sig_c & Sig_Z
```

交易 4 的输入来源于交易 3 的输出 $Sig_b \rightarrow Sig_Y$,即授权 $b \in Y$ 的最后一个交易。由于采用了分层钱包技术分配密钥且 $Z \supset Y$,因此通过 Z 的私钥 Zk 可以生成 Sig_Y 以完成交易 4。交易 5 是一个“自我交易”,该交易用于区分“授权交易”和“除权交易”。

2 个交易完整地记录了除权人 c 及其权限 Z 和除权时间等信息,并且除权阶段不需要被除权人的确认。

3.3.3　权限查询

权限查询不需要任何实体参与,仅凭区块链上的现有交易即可完成。

现假设需要查询 b 是否拥有权限 Y,流程如下:

```
if blockchain contains (Sig_b & Sig_Y→Sig_Y)
if no transaction after Sig_b & Sig_Y→Sig_Y
return true
return false
```

若 $b \in Y$,根据上文对授权操作的描述,区块链上必然存在交易 $Sig_b \ \& \ Sig_Y \rightarrow Sig_Y$,且不存在后续交易。

若 $b \notin Y$,存在 2 种情况:b 从未被授权 Y,链上不存在交易 $Sig_b \ \& \ Sig_Y \rightarrow Sig_Y$;$b$ 曾被授权 Y,链上存在交易 $Sig_b \ \& \ Sig_Y \rightarrow Sig_Y$。但后被除权,则根据除权过程的描述,必然存在后续交易 $Sig_c \ \& \ Sig_Z \rightarrow Sig_C \ \& \ Sig_Z$,其中,$c$ 为除权人。

由于区块链上查询交易的归属仅需公钥,当人物和权限实体公布公钥后,即可以根据当前链上的交易确定 b 是否拥有权限 Y。

3.4　物权转移

本文“物权转移”泛指供应链上的产品在不同的实体中交接的操作。与权限管理类似,物权转移的所有相关信息也会以交易的形式记录在区块链上。单品从供应链源头(代工厂)生产,至供应链末端(消费者)的流程可以分为生产和运输 2 个阶段,本节描述这 2 个阶段的流程设计。

3.4.1　生产阶段

生产阶段包含了单品 p_j 由代工厂 P_i 生产、通过质检并确认发货的过程,需要 2 个交易来记录,流程如下:

```
//代工厂 P_i 生产出产品 p 的一件单品 p_j,并进行质检
if p_j is qualified
//(pk,pK)衍生子密钥(p_jk,p_jK),分配给 p_j
derive key pair (p_jk,p_jK) from (pk,pK)
brand p_j with p_jK
//创建交易 1,记录合格产品的生产信息
create transaction None→Sig_P_i & Sig_P_i
//创建交易 2,记录发货信息
if verify (Sig_P_i) and verify (Sig_P_i)
create transaction Sig_P_i & Sig_P_i→Sig_S & Sig_T
else
destroy p_j
```

交易 1 是一个无输入的交易,表明了该单品的产地(代工厂)。在交易 2 中,Sig_S 为代工厂 P_i 发货部门权限的签名,Sig_T 为该单品接收方(如存储商)对接部门权限的签名。

3.4.2　运输阶段

运输阶段包含单品从供应链源头发出,经由中间环节运输至供应链末端的各个物权转移操作。该阶段实际上是单品在各个机构(储运商、零售商等)的内部供应链中流动,并交由下一个机构继续运输的过程。

现假设物权的当前归属为人物实体 $a_i \in A_i, i \in \{1,2,\cdots\}$,其中,$A_i$ 为 a_i 拥有的不同权限。转移的目标权限为 $B_j, j \in \{1,2,\cdots\}$。例如,现在单品 p_j 位于一辆多人负责的运输车上,下一阶段需要交由质监部门和仓储部门接收并入库。

根据下文即将描述的物权转移流程,当前区块链上存在交易:

$$Sig_{a_1} \ \& \ Sig_{a_2} \ \& \cdots \rightarrow Sig_{B_1} \ \& \ Sig_{B_2} \ \& \cdots$$

而后具有接收权限的人物实体 $b_j \in B_j$ 批准接收,并将后续的目标权限标记为 $C_t, t \in \{1,2,\cdots\}$。转移操作的流程为:

```
//b_j 向 Serv 发送物权转移请求
b_j request Serv with transfer Sig_a1 & Sig_a2 & ⋯ → Sig_B1 & Sig_B2 & ⋯
//Serv 验证 b_j 身份和权限
if b_j ∈ B_j for all j ∈ {1,2,⋯}
//Serv 使用 B_jk,将物权转移至 b_j
create transaction Sig_B1 & Sig_B2 & ⋯→Sig_b1 & Sig_b2 & ⋯
//b_j 批准转移,将后续转移目标设为 C_t
if verify (Sig_b1) for all j ∈ {1,2,⋯}
create transaction Sig_b1 & Sig_b1 & ⋯→Sig_C1 & Sig_C2 & ⋯
```

在 3.3 节描述的权限管控流程中,交易的输入

或输出是“人物实体 + 权限实体”混合签名的形式，而在物权转移阶段的相关交易中，不存在人物实体和权限实体在某一端混合的情况。因此，在权限管控和物权转移交易混合记录在一条区块链的情况下，不会造成交易表达信息的混淆。

当物权在外部供应链间转移时，交易也采用类似的流程构建。例如生产阶段最后的交易为 Sig_{P_j} & $Sig_{P_i} \rightarrow Sig_S$ & Sig_T，接收方负责人 $t \in T$ 和发出方负责人 $s \in S$ 共同确认交接完成后，双方构建如下交易即可完成物权转移记录的上链：

Sig_S & $Sig_T \rightarrow Sig_S$ & Sig_t

Sig_s & $Sig_t \rightarrow Sig_{N1}$ & Sig_{N2} & Sig_{N3} &…

其中，N_i 为接收方内部供应链的后续目标权限。

当物权转移到供应链末端实体时，利用“自我交易”将物权的最终归属改为实体本身即可。例如商品交易最终达成时，消费者 c 完成如下交易：

lastInput$\rightarrow Sig_c$

$Sig_c \rightarrow Sig_c$

该自我交易的两端都是人物实体，因此，不会和除权交易中的自我交易混淆。

3.5 产品溯源

由于所有物权转移的相关信息都以交易的形式记录在区块链上，因此本文方案中的产品溯源可直接以查询区块链交易的方式完成。

假设当前单品 p_j 的物权位于 x，x 可能为人物实体或权限实体。根据上文对物权转移的流程定义，区块链中必然存在交易：

$Sig_x \rightarrow Sig_{N_1}$ & Sig_{N_2} &…

其中，N_i 为后续目标人物实体或权限实体的签名（当其为供应链末端时为 Sig_x 本身）。

该单品的溯源流程如下：

```
transaction trans = Sig_x → Sig_N1 & Sig_N2 &…
while trans. input is not None
//查询前序交易
trans = lastTransaction( Sig_x → Sig_N1 & Sig_N2 &…)
//输出溯源信息
print extractPubKey (trans. input)
print trans. time
```

该流程实际上是一个不断查找前序交易的过程。这个过程提取所有参与 p_j 流动的实体签名，根据签名获取实体公钥，从而定位物权转移参与实体的相关信息。交易的时间戳即为物权转移的确认完成时间。

3.6 防伪验证

假设需要查询供应链源头为 P 的单品 p_j 的合法性，流程如下：

```
transaction trans = Sig_x → Sig_N1 & Sig_N2 &…
while trans. input is not None
//查询前序交易
trans = lastTransaction( Sig_x → Sig_N1 & Sig_N2 &…)
//提取代工厂 P_i 签名，获取公钥
publicKey = extractPubKey (trans. Sig_Pi)
if PK⇒P_iK
return true
else
return false
```

防伪验证的流程基于本文方案的 2 点特性：生产阶段的第一个物权转移记录为交易 $None \rightarrow Sig_{P_j}$ & Sig_{P_i}，因此，可以确定 p_j 的供应链源头为 P_i，并根据 Sig_{P_i} 获取公钥 P_iK；产品实体采用分层钱包技术分配密钥，因此，在没有生产商私钥 Pk 的情况下，仍然可以验证 $PK \Rightarrow P_iK$ 是否成立，即 P_i 是否为 P 认可的产地，由此判断 p_j 是否为一件合法的单品。

防伪验证的流程无需第三方参与，只需要生产商公布自己的公钥 PK 即可。

4 方案分析

4.1 秘钥分配

在现阶段，区块链技术已经逐步延伸到各个领域。同时，分层钱包树形结构密钥表达的组织层级关系，已经开始被应用于验证交易以外的用况。但在常规的区块链应用中，密钥仅作为人物实体的身份标识，用于生成标记交易的合法性的签名或数字证书。如文献[13]采用分层钱包技术，将个人的支付地址演化成一系列树状密钥簇，构建了一个抗攻击的匿名交易系统。文献[14]利用分层钱包技术的树状结构，提出了一种物联网智能家居应用领域上下级设备和应用的标记方式。

本文方案将供应链中的实体分为人物实体、产品实体和权限实体 3 类。人物实体的密钥相互独立，权限实体和产品实体密钥采用分层钱包技术分配。这种密钥分配方式是本文方案后续设计的基础，也是一种非对称加密密钥使用的创新。

产品实体的密钥分配分为 3 个阶段：

$(Pk, PK) \Rightarrow (P_ik, P_iK), i \in \{1, 2, \cdots\}$

$(Pk, PK) \Rightarrow (pk, pK)$

$(pk, pK) \Rightarrow (p_jk, p_jK), j \in \{1, 2, \cdots\}$

这 3 个阶段在编码上直接表达了产品实体的 3 个对应关系：代工厂 P_i 隶属与生产商 P，p 是生产商 P 的一个产品，p_j 是产品 p 的一个单品。由于分层钱包技术在密钥衍生上的唯一性和不可逆性，仅有父级密钥可以衍生出合法的子孙密钥用于交易签名。这种层级关系具有极高的稳定性和安全性，构成了本文方案产品溯源和防伪验证的基础。

本文方案将单品 p_j 的公钥 p_jK 作为 p_j 的唯一编码标识，这种利用分层钱包技术的编码方式可以广泛应用于物联网及相关领域。在常规的物联网编码体系（EPC、UID 等）中，实体的层级关系通过编码

的分段解析确定。例如在 EPC-96 中,64 位的编码被分为 8 位标头、28 位厂商识别码、24 位对象分类码和 36 位序列号 4 个码段。这种分段解析的方式,使很大一部分编码空间被用于描述“分层”信息(不同的版本号、不同的厂商、不同的对象等)。在本文方案中,层级关系直接在编码上表达,相对于传统编码体系节约了大量编码空间。并且,公钥对应的私钥可以用于满足某些需要加密的需求(例如本文方案中的防伪验证)。

传统编码体系的另一个局限是需要一个统一的管理机构(如 EPC global)分配码段,以保证编码的唯一性。这样虽然便于管理,但在一定程度上限制了用户的使用。在本文方案中,所有编码都由随机种子生成,用户使用安全的随机生成函数可以获得唯一的主密钥,不再需要统一的管理机构。

本文提出了人物实体与权限实体独立分配密钥的方式,该方式是本文方案权限管控的基础。在现有使用分层钱包技术的方案中,下级实体的密钥直接衍生自其附属的上级实体密钥,例如在文献[15]设计的智能家居系统中,传感器的密钥直接衍生自其上层智能网关的密钥

然而在权限管控领域,这种直接衍生的方式存在 3 个明显的缺陷:1)一旦上级人物实体密钥泄露,其下属所有实体的密钥将全部暴露,对系统安全带来灾难性的后果;2)如果人物实体的权限变动,需要重新为人物实体分配相应级别的密钥,非常繁琐;3)如何回收带有权限的人物实体密钥,在系统中将其标记为无权限或废止比较困难。

本文方案将权限实体从人物实体中独立出来,采用对人物实体“加权”和“除权”的方式表达人物的当前权限。该方式完全解决了上文描述的 3 个缺陷:由于人物实体的密钥相互独立,单一人物实体密钥的泄露、更换、授权和除权完全不影响权限体系的正常运行。权限实体的私钥保存在授权服务器内部,只公布其公钥,保证了方案的整体安全性。权限实体的密钥利用分层确定性钱包技术分配,利用密钥树的层级关系表达了权限的上下级关系。由于衍生函数的单向性,因此这种层级关系的安全性和稳定性在密码学上得到了完整地保护。

4.2　权限管控

本文方案提出一种基于区块链交易的权限管控方式,该方式的权限层级关系采用分层钱包技术确定,利用区块链技术保证权限管控体系的去中心化、安全性和公开性。

在现有的信息化系统中,权限管控是保证系统安全的重要核心之一。但无论是 Linux 系统内核[15],还是大型的 ERP 系统[16],其权限管控的相关信息都会被记录到一个经过加密的文件或数据库系统中,构成类似与“人物-权限”的键值对。

这种方式存在以下可改进的地方:首先,权限信息的不公开会造成独立系统间的交互困难,外界对于内部权限的验证需要专门的系统服务来处理。例如在供应链中,如果双方系统不提供相应的接口,生产商和储运商无法确认对方交接人员的权限信息,第三方人员也无法确认供应链参与人员实体的权限。其次,由于采用本地化存储,一旦保存权限信息的服务器出现故障,依赖于权限体系的所有业务逻辑都无法继续进行。并且,权限体系的安全性完全依赖于保存权限信息的服务器或数据库系统,一旦其被攻破,将对系统安全造成严重威胁。最后,权限管控的流程完全掌控在授权方,缺失了被授权方的确认流程。部分系统并不记录权限管控的详细信息(授权人、授权时间和授权人权限),会对问题回溯和责任定位造成困难。

本文方案在将人物实体和权限实体分别分配密钥的基础上,利用区块链技术提出了一种可以改进上述问题的权限管控体系。通过上文对“加权”和“除权”流程的形式化定义可以看到,方案中所有权限管控的信息全部以交易的形式记录在区块链上。由于区块链是一个去中心化的 P2P 系统,因此网络中任何节点都可以进行“权限查询”的流程,从而验证人物实体的权限信息。

相对于依赖于中心权限系统的传统系统,本文方案仅在进行授权和除权操作时需要授权服务器的辅助,权限查询操作不依赖于单一服务器。如果节点缓存有链上的相关交易,该操作甚至可在无网络环境下进行,数字签名算法保证了缓存数据的安全性和可验证性。由于在生产环境中,相对于权限查询操作,加权/除权操作仅占很小的一部分,因此本文方案降低了单一服务器的运行压力,具有很高的应用价值。

本文方案设计的权限管控体系的安全性不再依赖于某系统或数据库,而是由区块链及其底层的数字签名算法保证。以一个授权交易 Sig_a & $Sig_x \rightarrow Sig_b$ & Sig_Y 为例,该交易发起了一个 $b \in Y$ 的授权操作。由于有且仅有私钥 ak 和 Xk 可以生成签名 Sig_a & Sig_X,而 Xk 保存在安全的授权服务器内部,因此本文方案保证了授权操作的安全性(除权操作同理)。

现阶段已有一部分成果利用多重签名技术的优势解决多方交易的信任、安全等问题[17],但其主要目的在于验证交易的合法性,而非保存交易信息,提供系统记录的可溯源性。本文提出的这种以多重签名作为信息载体的方式,为多重签名技术的应用提出了一种新的方向。

在常规系统中,一旦保存权限信息的服务器或数据库被攻破,攻击者可以在无记录的情况下增加、

删除和篡改人物实体的权限,对整个权限体系造成严重破坏。在本文方案中,区块链的不可篡改性为权限信息存储提供了安全基础。由于链上交易不可篡改,不需要主动保护链中的授权和除权交易,即使在不安全的网络环境中,密码学也保证了权限信息的安全可靠。同时,由于区块链的可回溯性,即使在出现安全问题的情况下,也可以迅速进行排查和责任定位,防止危害进一步扩大,及时恢复权限系统的正常运行。

在本文方案中,在通过创建交易 Sig_a & $Sig_X \rightarrow Sig_b$ & Sig_Y 发起授权操作后,还需要被授权人通过交易 Sig_b & $Sig_Y \rightarrow Sig_Y$ 确认(或者说接受)该授权。这种“共同确认”的授权方式对被授权人来说既是一种保护(不会被强行授权),也是一种约束(授权确认后不可抵赖)。这是本文提出的一种新型权限管控模式,在进一步加强权限体系安全性的同时,也可以避免实际应用中很多权限相关的纠纷。

考虑到在实际应用中发起除权操作的人物实体不一定是授权阶段的授权人,因此,授权操作的最后一个交易 Sig_b & $Sig_Y \rightarrow Sig_Y$ 的输出为仅需要 Sig_Y,任何一个权限高于 Y 的人物实体 $c \in Z$ 都可以通过创建 $Sig_Y \rightarrow Sig_c$ & Sig_Z 来解除被授权人的权限。

4.3 物权转移

供应链中产品在实体间不断转移,信息化管控系统需要处理和记录这些转移信息,并保证记录的安全性。在常规系统中,这些信息被记录在一个中心式或分布式数据库内。但正如文献[18]指出,若采用中心式数据库系统,容易产生性能瓶颈,且当数据库出现故障时,整个系统将无法正常运行;若采用分布式数据库,则需要面对一些诸如数据冗余、一致性和系统可靠性等复杂的问题。本文方案利用区块链技术,在保证安全性的情况下,解决了供应链管控系统中的上述问题。

本文方案的物权转移信息完全以交易的形式记录在区块链上,利用多重签名技术使方案可以用于多方参与的转移过程。与权限管控类似,物权转移的流程需要交接双方的共同确认才能完成,解决了实际应用中因交接信息缺失而引发的纠纷。例如在快递行业中,经常出现的丢件、冒领。这种“共同确认”的特性既保护了交接双方的利益,也使交接记录完整地记录下来,出现问题时便于准确定位和追责。

在本文方案中,一次交接的过程需要“人物实体->权限实体”和“权限实体->人物实体”2 个交易来记录。考虑到实际应用中物权的转移并不总是发生在人物实体间。例如仓储部门的负责人在对产品进行清点入库时,还无法确定下个阶段负责运输的配送人员。因此,这种设计可以满足生产环境的实际用况,不会影响供应链本身的业务流程。

在常规的供应链管控系统中,物权转移的交接记录在数据库内部是“离散的”数据行。通过修改数据库内容,可以对供应链中某一环节的信息进行篡改。本文方案利用区块链记录所有物权转移信息,因此,交接记录具有完全的可回溯性,产品在系统内的流动无论是逻辑上,还是实际的数据存储都构成一个完整的链条。数字签名算法保证了链条的安全性,供应链的参与方无需主动保护物权转移信息,一旦物权转移操作被双方确认并记录上链后,该信息不可被篡改和删除。

由于区块链系统是一个 P2P 网络,对内部供应链而言,相较于中心式数据库,它提供了信息的去中心化处理和存储,解决了中心化架构中系统整体的性能和运行对于中心服务器的强依赖问题。相较于分布式数据库,区块链利用共识算法解决了一致性问题,利用数字签名算法为数据提供了有效性验证,降低了运维成本。

对外部供应链而言,P2P 网络架构打破了独立系统间数据交互的壁垒。现阶段由于系统间的异构性,跨内部供应链的数据交互需要双方提供统一的接口,构建贯穿多个孤立系统的高层次供应链管控解决方案存在很大困难。本文方案设计了内部供应链间物权转移的相应流程,多个内部供应链共享同一个区块链网络,利用数字签名算法等技术实现了安全的全网络信息共享。相较于常规系统,本文方案低成本、高效率地解决了供应链管控中由于系统间异构性造成的“信息孤岛”问题。

现阶段已经有一些采用区块链存储交易信息的系统出现。与本文方案相比,这些系统大多利用了一些新的区块链平台“记录除交易信息外的冗余数据”的特性。本文方案将所有物权转移的相关信息都以交易的形式记录下来。即使是比较原始的区块链平台,也可以完整实现一整套需求。同时,因为不需要高级功能的支持,不同区块链平台之间的转移和升级也变得相对简单,代码的基本逻辑不需要经历大的变动。

需要注意的是,区块链作为一个分布式的数据存储网络,比较适合记录内容简单且结构单一的数据,例如供应链中的物权转移信息。并且区块链系统的查询速度相对偏慢,因此,并不能完全替代分布式数据库。

4.4 产品溯源

现有的供应链管控方案由于独立系统的异构性,产品的全供应链溯源需要实现一个兼容供应链上所有平行系统间数据交互的高层数据平台,这会使平台的构造非常复杂,对平台本身的性能要求也

很高,需要耗费大量的经济和人力资源。

如上文所述,本文方案产品的流动在区块链上构成了一个完整且保证安全的链条,因此,可以根据该链条进行产品的溯源。根据方案对溯源流程的形式化定义,在供应链各参与方公布自己的公钥后,任何接入区块链网络的节点都可以对某件产品进行信息回溯。由于区块链的不可篡改性,从区块链交易链条中提取的回溯信息具有非常高的可信度,不存在常规系统中很容易发生的环节出现问题(例如信息丢失、恶意篡改或被攻击),导致整条供应链回溯信息可靠性受到影响。

本文方案中产品溯源所需信息的处理和存储成本由整个区块链网络共同承担,不再需要维护一个复杂度高、资源消耗大的高层数据平台,也无需担心数据存储的安全性,在不安全的网络环境、甚至离线的情况下,也可以获取到可靠的产品溯源信息。相较于其他系统,这是本文方案在产品回溯上的另一个优势。

4.5　防伪验证

本文方案利用分层钱包技术为产品实体分配密钥,不仅构建了一套完整的分层编码体系,而且也提供一种高效的防伪验证机制。

现行的防伪验证方案一般采用“验证码 + 验证平台”的方式,用户将产品标签上的验证码输入厂商维护的网络平台,从而获取产品的验证信息。这种方案存在如下缺点:1)验证码极易伪造和冒用,非法厂商在获取到一个合法的验证码后可大量用于同款产品的仿冒;2)对一个大产量的产品,维护一个需要响应大量验证请求的网络平台成本较高,一部分生产厂家难以承担;3)网络平台如果运行异常或被攻破,将会摧毁整个验证体系,甚至影响厂商和其他中间商的商业信誉。

本文方案单品的密钥衍生自其所属产品,产品和代工厂的密钥衍生自其厂商。同时,通过质检的单品在区块链中存有输入为“单品 + 代工厂”多重签名的交易。因此,在供应链的源头处会构成一个“厂商->代工厂->产品->单品”的树形结构,分层钱包技术中密钥衍生的单向性保证了该结构的安全和易于验证,非法厂商无法伪造单品的生产信息。在供应链中端或末端,由于用户可以查询到产品在整条供应链上的转移记录,因此不存在类似验证码冒用的问题。

与产品溯源类似,防伪验证信息的处理和存储成本也由区块链网络共同承担,并由数字签名算法保证验证过程安全可靠。相对与传统的验证体系,本文方案无论是对厂商还是对消费者而言,在经济性和安全性上都具有较大的优势。

5　结束语

本文结合区块链、比特币相关技术和多重签名技术,设计一套供应链管控和溯源方案。该方案将供应链内部实体分为“人物实体”“产品实体”和“权限实体”的分类方式,将分层钱包技术用于实体密钥的分配,并提出一种基于分层钱包技术的树形结构编码体系应用于物联网编码领域。通过设计基于区块链交易的去中心化权限管控机制和物权转移信息记录与验证机制,为利用区块链交易提供了新的思路。本文方案充分利用区块链和比特币技术去中心化、信息安全和记录可回溯等特性,解决了现有系统中一些常见的问题。下一步将根据该方案实现可用的系统框架与原型,逐步优化设计细节,以解决区块链记录信息速率较低等问题。

参考文献

[1] LAMBERT D M, COOPER M C, PAGH J D. Supply chain management: implementation issues and research opportunities [J]. International Journal of Logistics Management, 1998, 9(2): 1-20.

[2] STADTLER H. Supply chain management: an overview[M]. Berlin, Germany: Springer, 2015: 3-28.

[3] SEURING S. A review of modeling approaches for sustainable supply chain management [J]. Decision Support Systems, 2013, 54(4): 1513-1520.

[4] BEAMON B M. Measuring supply chain performance[J]. International Journal of Operations & Production Management, 1999, 19(3): 275-292.

[5] HUANG S H, SHEORAN S K, KESKAN H. Computer-assisted supply chain configuration based on supply chain operations reference model [J]. Computers & Industrial Engineering, 2005, 48(2): 377-394.

[6] YAN B, HUANG G. Supply chain information transmission based on RFID and internet of things[C]// Proceedings of IEEE CCCM'09. Washington D. C., USA: IEEE Press, 2009: 166-169.

[7] CHRISTOPHER M. Logistics & supply chain management[M]. [S.1.]: Pearson, 2016.

[8] 李志刚. 创京东:刘强东亲述创业之路[J]. 北京:中信出版社, 2015.

[9] BENTLEY L D, DITTMAN K C, WHITTEN J L. Systems analysis and design methods [M]. [S. 1.]: Irwin/McGraw Hill, 2000.

[10] SATOSHI N. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2017-05-30]. https://www.coindesk.com.

[11] COURTOIS N T, GRAJEK M, NAIK R. Optimizing sha256 in bitcoin mining [C]//Proceedings of International Conference on Cryptography and Security Systems. Berlin, Germany: Springer, 2014: 131-144.

[12] 沈厚才, 陶　青, 陈煜波. 供应链管理理论与方法[J]. 中国管理科学, 2000, 8(1): 1-9.

(下转第 101 页)

分词,因此占用了大量的内存以及 CPU 等主机资源,虽然 Reduce 任务仍在运行,但由于只是做简单的统计工作,对内存以及 CPU 等资源的需求并不是很高,由此集群资源开始回收,集群健康指数提升;在 170 个单位时间之后,Reduce 子任务执行阶段结束,标志 MapReduce 作业的完成,集群健康指数快速回升。通过分析可知,该模型在生产环境下能够有效检测集群评价指标的变化,并能够正确反映到集群健康走势图中。

由实验结果可以得出,本文提出的健康评价体系能够在指定时间段内准确反映集群的健康走势,管理员通过集群健康走势图可对集群的整体情况进行把控,大幅提升了工作效率,并且为整个 Hadoop 集群的持续健康运行提供了有效保障。

4　结束语

针对 Hadoop 集群中的安全隐患,本文设计了相应的安全加固方案,主要包括企业安全系统与 Hadoop 集群集成、字段级访问控制以及健康评价体系,并通过实验验证该方案的可行性与有效性。下一步将对健康评价体系的核心算法进行优化,以期更加精确地反映集群的健康状态,并结合机器学习为其提供预测能力。另外,由于版本的迭代,Hadoop 的安全问题会不断发生变化,下一步将继续研究 Hadoop 平台中的安全问题,并提出相应新的安全加固方案。

参考文献

[1] 高煜红. 云计算数据存储安全的研究[D]. 杭州:浙江工业大学,2014.

[2] NAIMI A I, WESTREICH D J. Big data: a revolution that will transform how we live, work, and think[J]. Information,2014,17(1):181-183.

[3] 孟小峰,慈　祥. 大数据管理:概念、技术与挑战[J]. 计算机研究与发展,2013,50(1):146-169.

[4] 何良均,张　翼,温宗臣,等. 一种多维度的 hadoop 权限控制方法和系统:CN 106250776 A[P]. 2016.

[5] 赵　妍,袁　野,刘　冰. 基于 LDAP 协议与 Kerberos 认证机制的统一认证[J]. 信息技术,2004,28(12):46-49.

[6] SALEH E, ALSA'DEH A, KAYED A, et al. Processing over encrypted data: between theory and practice[J]. ACM Sigmod Record,2016,45(3):5-16.

[7] BHANDARI R,KUMAR N,SHARMA S. Analysis of windows authentication protocols:NTLM and kerberos[EB/OL]. [2017-09-20]. https://www. researchgate. net/publication/265729617_Analysis_of_Windows_Authentication_Protocols_NTLM_and_Kerberos.

[8] 孙珊珊. 基于 Hadoop 的云计算数据安全性研究[D]. 武汉:武汉理工大学,2013.

[9] RATHOR V. 在 AIX 上用 LDAP 主-副本拓扑配置 Kerberos 主-从 KDC[EB/OL]. [2017-09-20]. https://www. ibm. com/developerworks/cn/aboutdw/page-not-available/.

[10] 陆松年,薛　质,蔡亦波. LDAP 与 Kerberos 系统的集成[J]. 计算机工程,2001,27(2):99-101.

[11] 章　松,刘春波. 基于 LDAP 的高可用目录服务器的设计与实现[J]. 软件,2015,36(12):146-148.

[12] GALLAGHER M J, NARASIMHAN V L. ADTEST: a test data generation suite for Ada software systems[J]. IEEE Transactions on Software Engineering,1997,23(8):473-484.

[13] 李　昊,张　敏,冯登国,等. 大数据访问控制研究[J]. 计算机学报,2017,40(1):72-91.

[14] 吴易雯,李莹杰,张列宇,等. 基于主客观赋权模糊综合评价法的湖泊水生态系统健康评价[J]. 湖泊科学,2017,29(5):1091-1102.

[15] 冯登国,张　敏,李　昊. 大数据安全与隐私保护[J]. 计算机学报,2014,37(1):246-258.

[16] 陈露露,郭文普,何　灏. 基于 ME-PGNMF 的异常流量检测方法[J]. 计算机工程,2018,44(1):165-170.

[17] 付亚男. 属性权重未知的多属性决策方法及应用[D]. 合肥:安徽大学,2014.

[18] GAO Y, NIE Y F. Traffic control management architecture based on Linux TC[EB/OL]. [2017-09-20]. http://en. cnki. com. cn/Article_en/CJFDTOTAL-SJSJ200620056. htm.

编辑　司森森

(上接第 93 页)

[13] MOSER M, BOHME R. Join me on a market for anonymity[C]//Proceedings of International Workshop on Privacy in the Electronic Society. Washington D. C., USA:IEEE Press,2016:123-132.

[14] ZHU X, BADR Y, PACHECO J, et al. Autonomic identity framework for the Internet of things[C]//Proceedings of 2017 International Conference on Cloud and Autonomic Computing. Washington D. C., USA: IEEE Press,2017:69-79.

[15] BOVET D P, CESATI M. Understanding the Linux kernel: from I/O ports to process management[M]. [S.1.]:O'Reilly Media,Inc.,2005.

[16] GRABSKI S V,LEECH S A,SCHMIDT P J. A review of ERP research: a future agenda for accounting information systems[J]. Journal of Information Systems,2011,25(1):37-78.

[17] 张　泓,曹珍富,董晓蕾. 基于承签原语与多重签名的改进虚拟交易系统方案[J]. 计算机工程,2016,42(2):137-141,145.

[18] MANEGOLD S,KERSTEN M L,BONCZ P. Database architecture evolution: mammals flourished long before dinosaurs became extinct[J]. Proceedings of the VLDB Endowment,2009,2(2):1648-1653.

编辑　索书志