Machine Translated by Google

短论文:设计与评估
基于公有链的隐私保护供应链系统

Takio Uesugi* 、Yoshinobu Shijo* 、Masayuki Murata**大阪
大学信息科学与技术研究生院 1–5 Yamadoka, Suita, Osaka, 565–0871 Japan 电
子邮件 :{t-uesugi, y-shijo, murata}@ist .osaka-
u.ac.jp

摘要:确保供应链中产品的可追溯性是一个紧迫的问题。最近,已经提出了使用公共区块链 (PBC)的供应链系统。在这些系统中,PBC被用作供应链各方之间共享的公共数据库,以确保所有权转让记录等分配信息的完整性和可靠性。因此,这些系统确保了供应链中的高水平可追溯性。然而,由于记录在PBC中的信息可以被任何人读取,所以分发信息可以是私人信息,但是是公开的。在本文中,我们提出了一种在使用 PBC 的供应链系统中保护隐私的同时确保可追溯性的方法。所提出的方法通过加密隐藏分发信息来保护隐私。此外,所提出的方法确保了合法供应链各方之间的分配,同时通过使用零知识证明来证明其真实性来隐藏其区块链地址。我们在以太坊智能合约上实现了所提出的方法,并根据交易费用评估成本绩效。结果显示,每方费用最多为2.6美元。

一、简介

供应链的快速全球化导致了严重的问题,特别是在可追溯性方面。经济合作与发展组织 (OECD) 报告称,2016 年国际贸易中的假冒产品总额达 5,090 亿美元,高于 2013 年的 4,610 亿美元[1]。

此外,由于供应链的复杂性,被大肠杆菌污染的食材无法追踪,导致2015年 Chipotle Mexican Grill爆发大肠杆菌疫情[2]。

为了解决这些问题,基于区块链的供应链系统被提出[3]-[5]。这些系统存储公共区块链 (PBC)中产品的分发信息。请注意,这些系统中的分配信息是所有权转移的记录。智能合约通过设置适当的条件来防止注册欺诈性分发信息。一旦信息存储在区块链中,由于其不变性,任何人都无法更改该信息。因此,这些系统确保了供应链中的高水平可追溯性。请注意,所有者是通过使用其区块链地址进行管理的。一般来说,区块链地址与现实世界的实体无关。因此,类似于公钥证书的机制用于将区块链地址链接到有关公司或个人的信息。

然而,这些系统存在隐私问题。分销信息是公司竞争优势的一部分,可能包括二级市场中个人之间的关系。因此,分发信息是需要保护的私人信息。然而,任何人都可以自由查看 PBC 中记录的信息。

结果,分发信息的隐私不受保护。

在本文中,我们提出了一种保护隐私的方法,同时确保使用 PBC 的供应链系统中产品制造商的可追溯性。传统方法无法保护隐私的主要原因是它们将区块链地址直接存储在区块链中。因此,所提出的方法通过使用制造商的公钥加密区块链地址来保护隐私

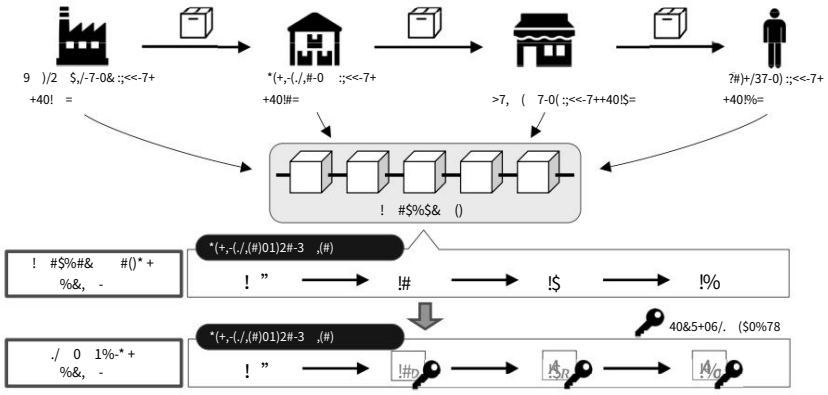

図 1. 传统方法和建议方法的概述。

Machine Translated by Google

将加密后的地址存储在区块链中,如图1所示。制造商可以使用自己的私钥解密地址来跟踪产品。为了消除非法方的分销,供应链各方（如图1中的M、D、R和C）必须在发货和接收产品时向系统表明他们是合法方。因此,所提出的方法使用零知识证明来允许供应链各方证明其真实性,同时隐藏其区块链地址。

为了评估所提出的方法,我们在以太坊平台上实施它。我们假设产品的分配或所有权的转移,从评估中的制造商开始。结果表明,所提出的方法可以保护隐私,同时确保制造商的可追溯性。我们还评估了分配的交易费用,发现每方的费用最多为 2.6 美元。

本文的其余部分结构如下。第二节讨论相关工作。第三节介绍了所提出的方法,该方法在第四节中在隐私性和可追溯性方面得到了验证。第五节描述了评估所提出方法的环境并介绍了评估结果。我们还提供了评估交易费用的结果。最后,第六节介绍了我们的结论和未来的工作。

二.相关工作

已经提出了几种基于区块链的系统来提高供应链中产品的可追溯性。

POMS [3] 是一个使用区块链管理产品所有权的系统,以防止在后供应链中流通假货。金等人。 [4]提出了一种通过重复消耗和生产可追溯资源单元（TRU）从材料阶段跟踪产品的方法。黄等人。 [5]提出了一种通过链下技术应用于高频配送的食品供应链的方法。然而,没有任何方法考虑保护分发信息的隐私。

三.提议的方法

我们提出了一种通过扩展 POMS 来保护分发信息隐私的方法 [3]。所提出的方法使用产品制造商的公钥来加密区块链地址。将这些加密地址存储在区块链中可以隐藏区块链地址并保护隐私。制造商可以使用自己的私钥解密并获取区块链地址列表来跟踪其产品。此外,供应链各方基于零知识证明证明,它知道只有合法供应链各方拥有的秘密令牌。因此,所提出的方法确保合法供应链各方之间的分配,同时隐藏其区块链地址。

所提出的方法由用于管理制造商信息的ManufacturerManager-Contract（MMC）、用于管理产品分发的ProductsManagerContract（PMC)和用于验证基于零知识证明的证明的VerifierContract（VC)组成。下面我们将介绍如何使用这三个合约来准备分销、注册产品、管理分销并跟踪产品。

A. 分发准备 为了准备分发,制造商信息被注册在MMC 中。所需信息是由制造商的区块链地址和公钥组成的一对。

如有必要,还可以注册其他信息,例如制造商的名称和电话号码。此外,MMC将制造商的区块链地址与其产品关联起来。

这些注册过程只能由指定的管理员执行。例如,这可以由 GS1 [6] 来执行,GS1 是一家制定和维护供应链全球标准的非营利组织。

B. 产品注册 只有在 MMC 注册的制造商才能作为产品的第一所有者向 PMC 注册其产品。在确认制造商已向MMC注册并与产品相关联后,制造商向PMC注册产品信息,从而启动产品的分发。下面,PMC用于管理所有权。

PMC 仅为制造商记录原始区块链地址,而不是加密地址。这是因为制造商想证明它已经制造了该产品。任何人都可以通过查看PMC中记录的第一拥有者来自由地识别该产品的制造商。

C、分销管理

图2说明了分发管理的流程。
配送管理包括以下八个步骤:步骤1至步骤4为发货流程,步骤5至步骤8为收货流程。

1) 所有者通过安全方法与接收者共享秘密令牌。

2) 所有者使用秘密令牌和制造商的公钥对接收者的地址AR进行加密以获得Enc(AR)。

3)所有者将VC部署在区块链上。
4) 所有者将接收者的加密地址Enc(AR)和步骤3得到的VC的合约地址记录在PMC中。

5) 接收者基于零知识证明生成一个证明,证明其知道步骤 1 中共享的秘密令牌。
6) 接收方将证明发送给PMC。
7) PMC 调用 VC 并验证发送的证明是否有效。
8) 所有者变更为Enc(AR)。

PMC 提供执行步骤 4、6、7 和 8 所需的功能。重要步骤解释如下。

首先我们解释一下步骤2中地址的加密。
我们使用椭圆曲线 elgamal 加密（如（1)中所示)来加密地址。

$$Enc(AR) = (kG, AR + kQ) \quad (1)$$

在所提出的方法中,k是秘密令牌,G是椭圆曲线的生成器， AR是接收者的地址,Q是制造商的公钥。注意， AR必须是椭圆曲线上的点才能加密。因此,我们使用从AR转换为椭圆曲线上的点的值。

Machine Translated by Google

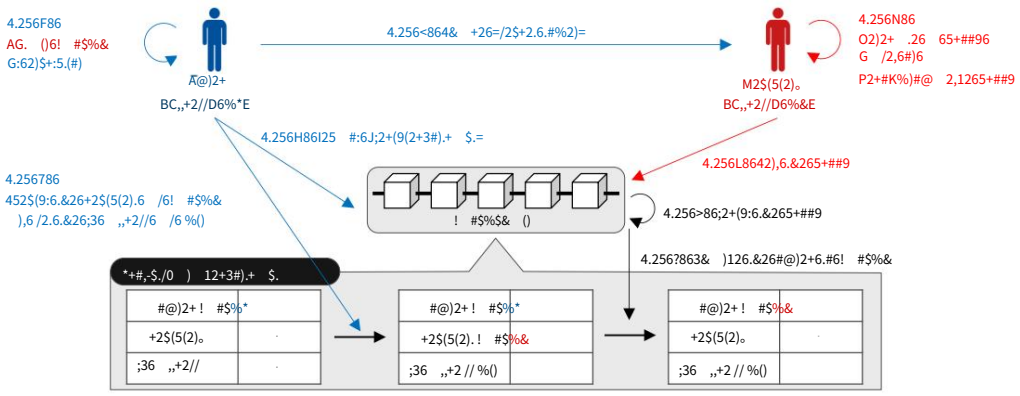

图2.所提出方法中的分发管理流程。

其次,我们描述第5步中的零知识证明。
为了计算接收者的加密地址Enc(AR),所有者和接收者必须知道(1)中所有的k、G、 AR和Q。虽然G、 AR和Q是公共信息,但k只有所有者和接收者知道。也就是说,只有知道k的合法所有者和接收者才能正确计算Enc(AR)。因此,接收方可以通过证明自己可以计算出Enc(AR)来证明自己是合法的。为此,我们使用零知识证明。零知识证明允许接收者证明其可以计算 Enc(AR) 而无需透露 k 和AR。尽管零知识证明有多种实现方式,但我们使用 zk-SNARK,由于其非交互性和小证明大小,已知它与区块链兼容 [7]。该证明在步骤 7 中得到验证。PMC 使用接收者的加密地址 Enc(AR)、制造商的公钥 Q 以及步骤 5 中生成的证明作为参数来调用 VC 来验证该证明。

实际上,即使在步骤4中,所有者在将接收者的加密地址记录在PMC中之前也证明其是合法的。这是为了防止合法所有者以外的任何人运输。与证明合法接收者的方式一样,所有者可以通过证明自己可以计算Enc(AO)来证明其合法性。

D、产品追踪

区块链记录了所有者的加密地址作为分配信息。它们使用制造商的公钥进行加密。因此,制造商可以通过使用自己的私钥解密并按时间顺序排列解密的地址来跟踪产品。

四.确认

我们验证所提出方法的可追溯性和隐私性
考虑攻击者的欺诈活动。

A、可追溯性

存在三种可能的攻击向量来抑制可追溯性。第一个是使用制造商的私钥干扰所有者加密地址的解密。攻击者可以使用制造商之外的公钥在区块链上记录加密语句来执行此操作。然而,第7步中的证明验证直接参考区块链中记录的制造商公钥来执行。因此,如果记录了用非制造商的公钥加密的语句,则步骤7中的证据验证总是失败。也就是说,攻击者的分发也失败。因此,这次攻击不可能成功。

第二个攻击媒介是不参与分发的第三方通过冒充所有者或接收者进行分发。如果第三方能够生成有效的证明,这种情况就可能发生。然而,由于零知识证明的健全性,那些不知道证明所需信息的人无法生成有效的证明。

因此,这次攻击不可能成功。

第三个攻击媒介是所有者和接收者之间的勾结,这使得难以识别所有者。攻击者可以使用除他/她自己的地址之外的随机或真实地址来执行此操作。除了秘密令牌之外,所有者和接收者还共享任意地址。通过使用它们生成证明,PMC 的所有者信息被正确更新。因此,这次攻击是有可能成功的。我们打算在未来的工作中应对这种攻击。

B. 隐私

攻击者可以通过从所有者的加密地址或 PMC 中记录的证明中检索地址来损害隐私。首先,我们考虑加密地址。

加密安全性取决于密钥长度和加密算法。例如,当使用254位椭圆曲线密码术时,不知道私钥的一方在实际时间内解密加密地址是极其困难的。因此,我们可以通过使用[8]中提出的254位椭圆曲线来确保该方法中加密地址的安全性。其次,我们考虑所提出的方法中使用的证明。我们在所提出的方法中使用了已知满足零知识性的零知识证明。换句话说,不可能从证明中恢复诸如地址和秘密令牌之类的信息。因此,攻击者无法损害隐私。

也就是说,攻击者无法检索所有者的区块链地址。

Machine Translated by Google

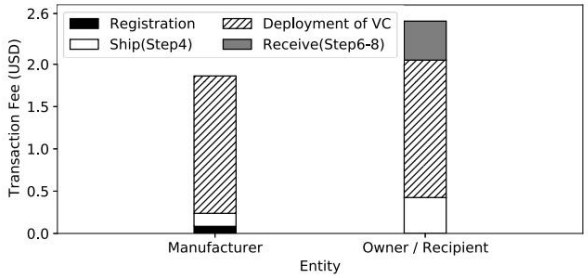

图 3. 特定产品的各方交易费用。

五、评价

为了评估所提出的方法,我们在以太坊平台上实施它。我们还衡量交易费用并根据评估结果讨论用例。

A. 环境设置

我们假设产品的分销从制造商开始。制造商执行产品注册和运输操作。其他方执行发货和接收操作。

我们使用 Solidity 版本 0.5.11 [9] 编写智能合约和 Remix [10] 提供的 JavaScript 虚拟机环境来评估所提出的方法。我们使用 ZoKrates [11]（zk-SNARK 的工具箱)来实现零知识证明。

B.结果与讨论

我们发现无法检索所有者地址
来自产品分发后记录在 PMC 和 VC 中的信息。我们还确认,制造商可以通过使用自己的私钥解密PMC中记录的所有者的加密地址来识别产品所有者。所提出的方法可以保护隐私,同时确保制造商的可追溯性。

我们测量了该分配的交易费用,并通过将 Gas 价格乘以 Remix 输出的 Gas 值将其转换为美元。截至评估时间为 2020 年 3 月 17 日上午 11:00（日本标准时间）,Gas 价格为每 Gas 1.1622 × 10−6 USD。该分布中各方交易费用的最大值如图 3 所示。

制造商和其他方有不同的交易费用,因为他们执行不同的流程。此外,根据是否使用零知识证明执行验证步骤,运输过程具有由制造商和其他方执行的功能的不同实现。因此,制造商和其他方之间运输过程的交易费用有所不同。

我们发现,一方所需的总交易费用最多为 2.6 美元。尽管通过优化实施还有降低费用的空间,但即使在目前的实施中,仍然有可以应用于汽车和家电等高价产品的用例。如果产品存在问题或缺陷,此类产品可能会被召回。召回面临的挑战包括提高消费者的召回意识和提高召回响应率[12]。

在通过所提出的方法进行分销的情况下,只有制造商可以跟踪产品。因此,这些问题可以通过跟踪需要召回的产品并通过立即通知所有者来召回该产品来解决。所有者最多支付 2.6 美元,即可及时实施产品维修或更换等措施。在这种情况下,交易费可以被视为获得这种保修的费用,我们认为2.6美元并不是昂贵的保修费用。

六.结论和未来的工作

在本文中,我们提出了一种方法,可以在使用 PBC 的供应链系统中保护隐私,同时确保产品制造商的可追溯性。我们在以太坊平台上实施了所提出的方法,发现每方的交易费用最多为 2.6 美元。

未来还有两个问题需要解决。第一个问题是考虑如何降低交易费用。该方法中的大部分交易费用来自 VC 的部署过程。制造商可以提前部署,而不是所有者为每个发行版部署 VC。如果供应链各方使用预部署的 VC,我们可以预期费用会大幅降低,因为只需一次性 VC 部署费用。如果交易费用可以降低,我们就可以将该系统应用到更便宜的产品上。第二个问题是扩展该方法,使其可以应用于产品的组装和拆卸。所提出的方法仅假设未经修改的单个产品的分布,即成品的分布。因此,如果它可以应用于产品的组装和拆卸,那么它就可以应用于成品以外的产品的分配。

参考

[1] 经合组织和欧盟知识产权局,假冒和盗版商品贸易趋势。经合组织出版,2019。

[2] 美国疾病控制与预防中心，“与 Chipotle Mexican Grill 餐厅相关的多州爆发的产志贺毒素大肠杆菌 O26 感染（最终更新）”,https: //www.cdc.gov/ecoli/2015/o26-11-15/index.html， 2016 年 2 月,[在线； 2020 年 3 月 17 日访问]。

[3] K. Toyoda、P. Takis Mathiopoulos、I. Sasase 和 T. Ohtsuki，“一种基于区块链的新型产品所有权管理系统 (POMS),用于后供应链中的防伪”,IEEE Access,卷。 5,第 17 465–17 477 页,2017 年。

[4] HM Kim 和 M. Laskowski，“面向供应链起源的本体驱动区块链设计”,会计、财务和管理中的智能系统,卷。 25、没有。 1,第 18-27 页,2018 年 3 月。

[5] 黄浩、周旭、刘建，“基于区块链和EPC技术的食品供应链溯源方案”,载《智能区块链论文集》,2019年,第32-42页。

[6]《GS1 |全球商业语言”， https://www.gs1.org/， [在线； 2020 年 3 月 17 日访问]。

[7] AM Pinto，“区块链中 zk-SNARK 的使用简介”,《区块链经济数学研究论文集》,2020 年,第 233-249 页。

[8] B. WhiteHat、J. Baylina 和 M. Bell´es，“Baby jubjub 椭圆形 https://iden3-曲线，” docs.readthedocs.io/en/latest/ downloads/ [在线；33717d75ab84e11313cc0d8a090b636f/Baby-Jubjub.pdf，2020 年 3 月 17 日访问]。

[9]“Solidity”， https://solidity.readthedocs.io/， [在线； 3 月 17 日访问 2020]。

[10]“Remix - 以太坊 IDE”， https://remix.ethereum.org， [在线； 2020 年 3 月 17 日访问]。

[11]“ZoKrates”， https://github.com/Zokrates/ZoKrates， [在线； 2020 年 3 月 17 日访问]。

[12] 经合组织，“增强全球产品召回有效性”,经合组织科学、技术和产业政策文件,第 1 期。58,2018 年 11 月。