使用双区块链的防伪溯源系统

刘家稷, 杨 挺, 汪文勇

电子科技大学 计算机科学与工程学院 成都 中国 611731

摘要 区块链是一种随着比特币等加密货币而兴起的一种类似于非关系型的分布式存储数据库, 本文利用区块链分布式存储、去信任化和不可篡改的特性设计了一个基于区块链技术的防伪溯源系统(Traceability System Using Public and Private Blockchain, TSPPB)。TSPPB 使用公有链和私有链两套区块链, 该溯源系统能够确保获得的溯源信息的真实可靠不可篡改并解决传统产品溯源系统存在的产品标签复制、滥发和产品质量问题相关责任人及问题环节定位困难的问题。在确保溯源信息安全性并解决传统溯源系统隐患的同时, TSPPB 还能够高效且保持低成本的运行。

关键词 溯源; 区块链; 不可篡改; 责任人
中图法分类号 TP391 DOI 号 10.19363/j.cnki.cn10-1380/tn.2018.05.03

Traceability System Using Public and Private Blockchain

LIU Jiaji, YANG Ting, WANG Wenyong

Computer Science Academy, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract Blockchain is a non-relational distributed storage database that arises along with bitcoin and other Encryption currency. This paper designs a traceability system based on distributed storage, de-trusting and non-tampered characteristics of blockchain. Our traceability system uses two sets of block chain systems, the public chain and the private chain. Our traceability system can ensure that the database of product traceability system can't be tampered, solve the problem of product replication, over issue and bind the person responsible to their product quality problem. Our traceability system can ensure the efficient and low cost operation of the traceability system at the same time.

Key words traceability; blockchain; non-tampered; responsible

1 引言

区块链是一种类似于非关系型数据库这样的技术解决方案。其具有不可篡改、去信任化、分布式存储和强抗损性等特性。本文利用区块链的上述特性, 设计出了一种基于区块链技术的溯源系统(Traceability System Using Public and Private Block-chain, TSPPB)及相关协议。本文将在第 2 节介绍区块链技术, 在第 3 节中, 本文将给出溯源系统的协议设计, 并在第 4 节证明该协议的安全性。本文的第 5 节将利用该协议设计一个基于区块链技术的防伪溯源系统(Traceability System Using Public and Private Blockchain, TSPPB)。

产品溯源是现代供应管理的一种重要手段, 随着食品安全等问题受到政府与社会大众的关注, 产品溯源(如食品、农产品安全溯源)领域的信息应用技术正快速发展。产品溯源[1]的信任问题是传统技术一直期望解决的问题, 因此, 基于区块链技术的产品溯源系统应运而生。与多数新兴的基于区块链技术的溯源系统不同, 本文所述的 TSPPB 使用公有链和私有链两套区块链系统, 能够有效的解决信任和效率之间的平衡问题。

目前主流的产品溯源系统主要是由政府相关部门或者某个核心企业为中心并主导, 利用行政手段或市场地位强制在上下游相关企业按照其规范配合使用。产品的溯源记录由某个部门或公司进行处理。

这种传统的产品溯源系统存在以下隐患: 1.产品溯源系统的数据库从技术上无法避免篡改产品信息。2.正品的标签信息可被赝品复制。3.产品如果出现质量问题, 问题环节以及相关责任人定位困难。4.生产

通讯作者: 杨挺, 博士, 讲师, Email: yting@uestc.edu.cn。
本课题得到: 四川省科技厅“基于区块链的物联网溯源综合平台项目”(项目编号 2018GZ0218)以及国家电网公司科学技术项目“新能源厂站网络安全防护关键技术研究”(项目编号 522722180007)资助。
收稿日期: 2018-01-31; 修改日期: 2018-05-08; 定稿日期: 2018-05-02

方可超出应有产量随意滥发产品。

为解决上述溯源信息被篡改的隐患, 相关研究者与科技公司提出了基于区块链技术的溯源方案。Abeyratne[2]展望了将区块链技术应用于供应链管理的远景, 并分析了在供应链管理中可能会遇到的问题。Regattieri [3]分析食品溯源的的法律和监管的问题。Huertas [4]讨论了如何在其设计的 Eximchain 上使用智能合约来进行供应链管理。

目前有几种基于区块链技术的设计, 如 Feng Tian[5]构建了一个基于 RFID 技术与区块链技术的溯源系统 Agri-food Supply Chain Traceability System, 以防止溯源系统的信息被篡改并用于防止标签复制, 引入了 BigchainDB[6]的概念, 以解决区块链需要存储现实世界中的大量数据时可能存在的扩展性不足的问题。沃尔顿链[7] 是一种结合了 RFID 技术与区块链技术的溯源系统, 防止溯源系统的信息被篡改并通过 RFID 防止标签复制。沃尔顿链[22]的通过母链子链能够实现溯源功能。其中, 子链本身针对具体的应用场景, 可以开发不同的智能合约来满足各种应用需求, 并在具体的技术细节上可以针对性更改(如采用不同的共识机制), 母链用于管理子链。

Eximchain、沃尔顿链、Agri-food Supply Chain Traceability System 等使用区块链技术的溯源系统都使用自己搭建的区块链来存储产品的溯源信息, 其安全性基于自身系统搭建的区块链系统来保证安全性, 由于这些溯源系统所搭建的区块链无法获得接近比特币或以太坊这种流行的区块链的算力, 因此它们的安全性必然弱于以太坊或比特币等拥有庞大算力保证的区块链。但是, 直接采用比特币和以太坊区块链等公有链技术的溯源系统却面临着效率低下、信息存储量小、开销高等问题。

与上述基于区块链的溯源系统类似, 本文所述的 TSPPB 能够提供真实可靠的溯源信息、保证溯源系统的高效运行以及控制成本。与此同时, TSPPB 还解决了产品的标签复制和滥发等问题。TSPPB 与上述的溯源方案不同之处在于, 为保障私有链中存储数据的安全性, TSPPB 将私有链中的数据与拥有庞大算力保证的公有区块链(如以太坊或比特币等)进行关联, 用公有链中数据的不可篡改性来确保私有链系统中存储数据的不可篡改性。同时, TSPPB 通过 TCDBB 技术解决产品的标签复制和滥发问题, 不需要使用 RFID。

为减少存储在私有区块链中的数据的复杂度, 在 TSPBB 中, 私有链将只存储溯源信息的哈希值, 详细的溯源信息将存储于 5.4 节所述的 IPFS 系统中, 而不需要专门构建类似于 BigchainDB 的系统。

由于 TSPPB 采用区块链来存储溯源信息, 并且每个存储溯源信息的区块都会有区块号, 故 TSPPB 能够记录每个溯源信息加入溯源系统的时间, 精度与公有链区块时间发布一致。能够用于记录产品的各生产阶段时间。

2 区块链技术

区块链是一种类似于非关系型数据库特点。区块链由若干区块构成, 每个区块存储若干交易数据(消息)。每条消息的数据和区块中已处理的消息进行哈希计算(Hash Function, 也称为散列函数), 获得相对应的哈希值并利用 merkle tree[8]的数据结构将这些消息以及消息的哈希值存储在区块中。

根据区块链的应用场景, 区块链可以分为以下几类:

1. 公有链: 任何人都以生成交易或查看区块链状态。每笔交易都可由 PoW, PoS, DpoS[9]等共识机制进行确认。

2. 联邦链: 只有组织的成员才能连接到区块链, 并生成交易或查看区块链状态。交易由共识机制进行确认。

3. 私有链: 只有企业内部可以使用区块链。一般用于企业, 提供安全、可追踪、自动化的平台。

通常来讲公有区链(如比特币区块链, 以太坊等)可信度高, 但存储效率低且费用较高。私有区块链与公有区块链相比, 是一种高效、大容量的信息存储方式, 因此本文结合二者优缺点设计了一种包含公有区块链与私有区块链的防伪溯源系统。

本文利用区块链的安全性设计基于区块链技术的溯源系统(TSPPB)。TSPPB 的安全性基于区块链自身的安全性。区块链的安全性基于以下特征[9]:

1. 去信任化

去信任性即参与系统的每个节点之间进行数据交换是无需相互信任的。在 TSPPB 系统中, 生产过程中的各部门会作为节点接入私有链, 利用区块链去信任化的特征, 防止系统受到恶意节点的攻击。

区块链的分布式记账技术体现在所有存储数据对系统内节点的公开化与一致化, 类似于一个公开透明社会的“征信”系统, 它打破了社会信息的不对称、不可信的僵局。上述特征被称为“去信任化”。

区块链的去信任化有赖于拜占庭一致协议所具有的鲁棒性和抗攻击能力, 实现对异常行为的发现和保证数据的全网一致性。

拜占庭一致协议实现如下功能: 在 n 名成员构成的系统中, 如果成员中的叛逆者(攻击者)数目为 t, 那么只要 n>3t 则在同步通信网络环境下能够保证:

(1) 在有限时间内终止协议。

(2) 忠诚一方最终达成一致结果。

2. 分布式存储

区块链本质上是一个分布式存储系统, 有别与一般的分布式数据库系统, 区块链技术采用分布式记账模型, 该模型与传统分布式数据库的显著区别在于如下三点:

(1) 传统分布式数据库系统支持“增加、删除、修改、查询”四种操作, 而区块链只有“增加”和“查询”两个操作。

(2) 区块链由一系列数据区块构成, 每个区块由包含元数据的“区块头”以及包含当前周期内多条交易记录的“区块体”构成。这种结构更加安全, 其原因在于其由两种带密码学哈希机制的数据结构组成:哈希链表, merkle tree[8]。由着两种数据结构来组成区块链可以很快发现区块数据的篡改。

(3) 与传统数据库相比, 第 2 点中的存储方式提供了对交易数据一致性检验和完整性检验的功能的支持。

由于在 TSPBB 中, 不同溯源信息需要由不同参与节点添加, 溯源信息可以考虑采用分布式存储的方式构建, 但需要确保信息的可信度。而采用区块链存储数据, 可以全网同步的检测到数据的更改。所以使用区块链存储溯源记录可以防止溯源记录被更改, 即可以确保溯源信息的不可篡改性。

3. 强抗损性

区块链是由多个节点通过共识机制组成的分布式记账系统, 任意小部分节点的损坏或失去都不会影响整个系统的运行。利用该性质设计基于区块链技术的溯源系统可提高系统的抗损性。

3 溯源协议

3.1 溯源协议设计

本文设计了一种基于区块链技术的溯源系统(Traceability System Using Public and Private Blockchain, TSPPB)及相关协议。与一般的基于区块链技术的溯源系统不同, TSPPB 将使用公有链和私有链两套区块链系统。在 TSPPB 中, 私有链存储对各个部门对产品的溯源记录, 公有链中存储产品所有溯源信息的哈希以完成对产品溯源信息的校验功能。

私有区块链与公有区块链相比, 是一种高效、大容量的信息存储方式; 而公有区块链可信度高, 但存储效率低且费用较高。因此, 本文使用两种方式相辅相成, 构成一种实用的溯源方案。

在本文中公有区块链可以是企业或组织自行创建自行维护的区块链, 也可以采用诸如以太坊等成熟且拥有众多节点的系统, 增强溯源系统的可信度。私有链为需要企业自身创建并维护。企业的各个部门可将生产中各个环节的数据存储在私有链中并将这些信息生成标签信息存储在公有链中作为公正。

如图 1 所示, 在本文所述源协议中, 对于某产品, 策划部门 Pl 将向私有链加入的生产计划, 该信息包括:

1. 产品的生产计划 P。

2. 相关负责人的数字签名 Si_{Pl}。

3. 生产计划 P 通过哈希运算生成的标签信息。

P	Si_{Pl}	H(P)

图 1 策划部门加入生产计划格式

Figure 1 The format of Production Planning

如图 2 所示, 其他各部门将向私有链中加入该部门负责的溯源信息, 该信息包括:

1. 生产过程中各生产流程产生的信息 M(包括溯源信息及产品编号)。

2. 该部门相关负责人数字签名 Si(为了能够追溯产品质量问题的相关责任人, 需要添加相关部门签名)。

3. 产品生产信息通过哈希运算生成的标签信息 H(M)。

M	Si	H(M)

图 2 各部门加入溯源信息的格式

Figure 2 The format of traceability information

如图 3 所示, 销售部门 X 加入的溯源信息包括:

1. 私有链中该产品生产过程中所产生的所有标签值做哈希运算生成该产品的标签。

2. 产品的 ID。

3. 销售部门的数字签名Si_x。

在生产流程的最后一个部门完成对私有链的存储操作时, 销售部门 X 将私有链中该产品生产过程中所产生的所有标签值(溯源信息的哈希值以及各个部门的哈希$\mathrm{H}(M_i, Si_i)$)做哈希运算生成该产品的标签$H_{PR} = H(\mathrm{H}(M_1, Si_1), \mathrm{H}(M_2, Si_2) \ldots)$ 并将其存储到公有链中。对每一件产品, 销售部门 X 都会生成一个该产品的 ID, 并将销售部门的数字签名Si_x发送给公有链。若数字签名合法, 公有链将该 H(ID)存储在公

有链中。对每一件产品, 销售部门会为其生成一个链接 T, 该链接用于在私有链及公有链中查询产品溯源信息。

ID	Si_x	H (H(M_1,Si_1), H (M_2,Si_2), ..., H(M_n, Si_n),H(P))

图 3　销售部门加入溯源信息的格式

Figure 3　The format of sales information

定义销售信息(包括销售时间)S。在销售产品时, 销售节点将销售信息 S 及该节点的数字签名Si_x发送给公有链, 公有链判定数字签名是否合法, 若合法则将销售信息存储在公有区块链系统中。销售信息, 包括销售时间、销售地点、销售人和经销商等信息。这些信息可防止复制, 即同一产品不可能消费两次。

消费者可通过公有区块链, 获取产品的标签信息和销售信息。消费者、质检部门和其他相关人员都能够在私有区块链位置上获得详细的生产信息, 并通过该产品的标签信息对所获得生产信息进行校验以完成产品的溯源。

3.2　溯源数据的记录查询与校验

各个部门加入溯源信息的过程如图 4 所示, 各个部门需要向私有链中加入溯源信息, 自己对溯源信息的签名以及上述两者的哈希值。

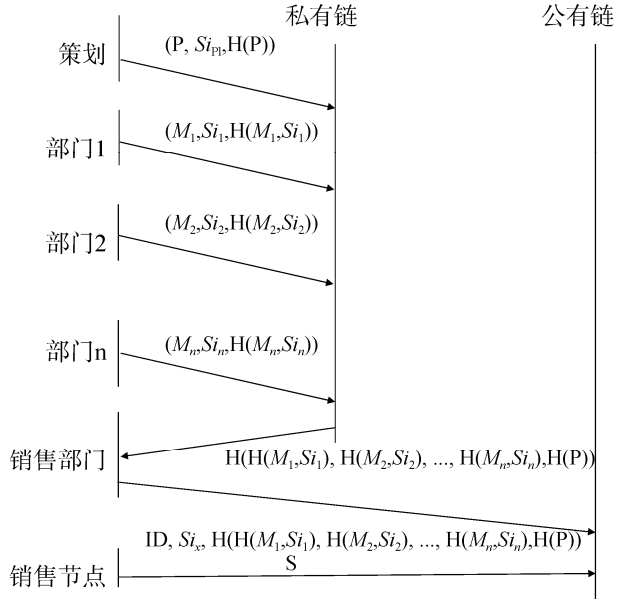


图 4　溯源数据记录

Figure 4　Record traceability information

定义策划部门为Pl, 生产过程中的各个部门为 D_i , Pr 表示私有链, Pu 表示公有链, Cl表示查询客户端, X 表示销售部门, Sa 表示销售节点, M_i 表示产品生产过程的详细信息, h 表示公有链中存储的详细信息的哈希值, h1 表示公有链中存储的ID 的哈希值, s 表示销售信息。Tag 为产品标签, 分别包含该产品在公有链和私有链中信息的连接L_{pr}, L_{pu}以及 ID 数据。

溯源记录包括以下步骤:

1. 策划部门提出生产计划 P, 计算出生产计划的哈希 H(P)并签名该计划($Si_{pl} = Pl.\mathrm{sign}(H(\mathrm{P}))$)。

2. 策划部门将生产计划 P 及其签名Si_{pl}和生产计划的哈希 H(P)存入到私有链中。

3. 各生产部门将生产过程中产生的信息($M_1, M_2, \cdots$, 如产品编号、生产计划、检测数据、农药品种和使用数据、种苗、物候、产地信息和物流过程信息等各阶段的数据)构建区块, 存储于私有区块链中, 并对这些数据进行签名, 生成哈希存储于私有链中。

4. 对于每件产品, 销售节点将 产品 ID、私有区块链中对应信息的哈希值H_{pr}以及销售节点的签名Si_x构建可验证的标签信息并将其存储于公有链中。

5. 经销节点将产品的销费信息 S(包括销费时间和销费地点)及该对信息的签名Si_x加入到公有区块链中。

上述步骤用伪代码表示如下:

算法1.溯源数据存储

输入: 某产品的生成计划P以及各溯源部门的溯源信息$M_1, M_2, \cdots, M_n$。私有链及公有链中没有该产品的信息。

输出: 对于每一件产品, 私有链存储该产品的生产计划 P 及各部门的溯源信息M_i, 各部门的签名Si_i以及这些信息的哈希值H(M_i, Si_i), 公有链存储上述信息的哈希值 H(H(M_1, Si_1), H(M_2, Si_2), ...)。每一件产品其详细信息在私有链中的位置会存储到一个链接L_{pr}中, $H_{PR} = H(\mathrm{H}(M_1, Si_1), \mathrm{H}(M_2, Si_2), \ldots)$在公有链中的位置将会存储到另一个链接$L_{pu}$中。

过程 1.存储溯源数据

BEGIN

Pl.*generrate*(P);

Si_{pl} =Pl.*sign*(P);

h_p =H(p);

Pl.*send*(p, Si_{pl}, h_p ,Pr);

//发送者为策划部门接收者为私有链

for(i = 0 ; i<D. size(); ++i){

D_i.*generate*(M_i);

Si_i=D_i.*sign*(M_i);

$h_{M_i} = \mathrm{H}(M_i)$

D_i.send(M_i, Si_i, h_{M_i},Pr);

}

$h = H(\sum h_{M_i}|Si_{pl})$;

Pr.send(h,X);

X.*generate*(ID);

h_{ID}=H(ID);

X.*send*(ID, L_{Pr}, L_{Pu},Tag);

X.*send*(ID, h, Si_x, Pu);

Sa.*genrrate*(S);

Si=Sa.*sign*(S);

Sa.*send*(S, Si, Pu);

END

各部门获得溯源信息的过程如图 5 所示, Cl 通过 Tag 分别获得该产品在公有链和私有链中信息的连接L_{pr}和L_{pu}。使用上述链接查询产品溯源信息并判断溯源信息的真实性。

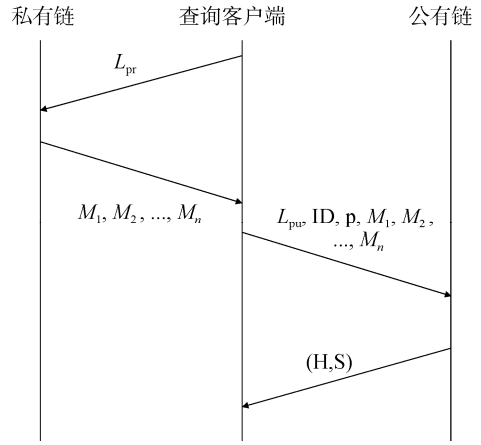


图 5 溯源数据获取与验证

Figure 5 Get traceability information and verify

消费者或相关质检部门由产品标签获得产品溯源信息, 其验证方法包括以下步骤:

1. 获得Tag, 并由Tag获得该产品在公有链和私有链中信息的连接L_{pr}, L_{pu}和ID。

2. Cl由(L_{pr})在私有链中查询该产品信息。

3. Cl根据(L_{pu}, ID)在公有链中查询该产品信息。

4. 根据产品在公有链中的标签信息和私有链中的详细生产信息是否匹配确定该产品的真实性。即验证公有链中存储的产品标签信息H_{pr}, 与私有链中存储的产品在各生产步骤中的详细信息: ($M_1, M_2, ..., Si_1, Si_2, ..., P, Si_c$)是否满足: $H_{PR}=H(\sum H(M_i,Si_i)+H(P,Si_c))$

若满足,则私有链中存储的信息为真。

5. 公有链根据产品在公有链中的相关销售记录S 确定该产品的唯一性。

上述步骤用伪代码表示如下:

算法2. 溯源数据查询

输入: 某产品的Tag包括 L_{pr} , L_{pu} 以及ID

输出: 该产品的详细溯源信息

过程 2. 溯源信息查询

BEGIN

get(L_{pr} , L_{pu} ,ID, Tag);//由 Tag 获得 L_{pr} , L_{pu} ,ID

Cl.*send*(L_{pr} ,Pr);

Pr.*send*($M_1, M_2, ..., M_n$,P,Cl);//从私有链中获得信息

Cl.*send* (L_{pu} , $M_1, M_2, ..., M_n$, P, ID, Pu); //将信息送往公有链验证

IF(! $H_{PR} = H(\sum H(M_i, Si_i) + H(P, Si_c))$)

return error; //数据篡改或仿冒

Pu.*send*(S,Cl); //从公有链获得销售信息

END

在本文所述的溯源协议中, 消费者、质检部门和其他相关人员都能够在私有区块链位置上获得详细的生产信息。

取证人员可以通过公有区块链的哈希值、产品编号等信息与对应的私有区块链的数据进行检查, 确认私有区块链数据是否被恶意篡改。若有篡改, 则私有区块链对应的哈希值与公有区块链中对应的哈希值不同。

4 溯源方案安全性讨论

对于第 3 节中描述的溯源协议, 我们需要确保私有链中存储的产品各生产过程的数据确实由生产过程中的相关部门添加, 且数据不可篡改。确保公有链能对产品信息的真实性, 查询的合法性进行验证。

TSPPB 溯源系统在公有链中所存储数据的安全性基于公有区块链本身所具有的安全性, 即由公有区块链的不可篡改性可以保证存储到公有区块链系统中数据的不可篡改性。故我们不对存储在公有链中数据的安全性进行讨论。

为证明第3 节所述的溯源协议的安全性, 即需要证明该协议能够保证溯源信息由相关责任部门加入, 且溯源数据没有被篡改。我们定义表 1 所示符号[10]并利用表 2 所示引理来对本文所述的溯源协议的安全性进行证明[10]。

表 1 符号定义

Table 1 The definition of symbol

符号	含义
p ◁ X	P 接收到信息 X
P ∋ X	P 拥有信息 X
H(X)	X 的哈希值
-K	私钥
+K	公钥
$\{X\}_{-K}$	X 被一个私钥-K 加密得到的值
Q|~X	Q 传达过信息 X
P| ≡ X	P 相信表达式 X 为真
$P\| \equiv \overset{+K}{\longrightarrow} Q$	P 相信+K 为 P, Q 通信的公钥
P| ≡ ϕ(X)	P 认为 X 可被验证
(X,Y)	X,Y 信息的组合

表 2 引用结论

Table 2 Some inference

编号	条件	结论
R6	P ∋ H(X)	P| ≡ ϕ(X)
I4	$p \lhd \{X\}_{-K}, P \ni +K, P\| \equiv \overset{+K}{\longrightarrow} Q, P\| \equiv \phi(X)$	P| ≡ Q|~X, P| ≡ Q|~$\{X\}_{-K}$
P4	P ∋ X	P ∋ H(X)
P1	p ◁ X	P ∋ X
P3	P∋ (X, Y)	P∋ X

在本文所述的溯源协议中数字签名Si表示各个部门用其私钥对生产信息进行加密, 即

$$Si_i = \{M_i\}_{-K_{D_i}}, Si = \{S\}_{-K_{Sa}}, Si_c = \{P\}_{-K_{Pl}} \quad (V1)$$

其中, $-K_X$ 表示X部门私钥。

公有链中存储有 $H(\sum H(M_i, Si) + H(P))$ 即:

$$Pu \ni H(\sum H(M_i, \{M_i\}_{-K_{D_i}}), H(P, \{P\}_{-K_{pl}})) \quad (V2)$$

其中, $\sum H(M_i, \{M_i\}_{-K_{Di}})$ 表示: $\sum H(M_1, \{M_1\}_{-K_{D1}}), \sum H(M_2, \{M_2\}_{-K_{D2}}) \ldots \sum H(M_n, \{M_n\}_{-K_{Dn}})$

加入产品 ID 的第四步可表示为:

$$Pu \lhd ID \quad (V3)$$

加入生产信息的第五步可表示为:

$$Pu \lhd S, \{S\}_{-K_{Sa}} \quad (V4)$$

查询生产信息的第二步可以表示为:

$$C \lhd \sum M_i, \{M_i\}_{-K_{D_i}} P, \{P\}_{-K_c} \quad (V5)$$

在V5中, $\sum M_i, \{M_i\}_{-K_{D_i}}$ 表示: $M_1, \{M_1\}_{-K_{D_1}}$, $M_2, \{M_2\}_{-K_{D_2}}, \ldots, M_n, \{M_n\}_{-K_{D_n}}$

由于公有区块链具有极高的可信度, 所以对于查询客户端 C 而言, 从公有链中获得的数据可信, 故有:

$$C \ni H(\sum H(M_i, \{M_i\}_{-K_{D_i}}), H(P, \{P\}_{-K_{pl}})) \quad (V6)$$

各个部门的公钥是公开的, 故可以认为:

$$P \mid\equiv \xrightarrow{+K} Q, P \ni +K$$

对任意 P, Q 均成立, 即:

$$Pu \mid\equiv \xrightarrow{+K_x} X, Pu \ni +K_x \quad (V7)$$

$$Pu \mid\equiv \xrightarrow{+K_{pa}} Pa, Pu \ni +K_{Pa} \quad (V8)$$

$$C \mid\equiv \xrightarrow{K_{D_i}} D_i, C \ni K_{D_i} \quad (V9)$$

$$C \mid\equiv \xrightarrow{K_{Pl}} Pl, C \ni K_{Pl} \quad (V10)$$

我们需要协议满足 V14, V15, V16, V17 和 V18 即:

产品各生产过程的数据确实由生产过程中的相关部门添加。即:

产品销售信息确实由某个销售节点加入。即:

$$Pu \mid\equiv Pa \mid\sim S \quad (V14)$$

$$C \mid\equiv D_i \mid\sim M_i \quad (V15)$$

生产计划由策划部门Pl添加。即:

$$C \mid\equiv Pl \mid\sim P \quad (V16)$$

可验证D_i, P及数字签名是否被篡改。即:

$$C \mid\equiv \Phi(M_i, \{M_i\}_{-K_{D_i}}) \quad (V17)$$

$$C \mid\equiv \Phi(P, \{P\}_{-K_{Pl}}) \quad (V18)$$

表 3 安全性推理

Table 3 Safety inference

标号	结论	论据
V11	$Pu \ni S, ID, \{S\}_{-Ksa}$	V4,P1
V12	$Pu \ni H(S)$	V11,P4
V13	$Pu\| \equiv \phi(S)$	V12,R6
V14	$Pu\| \equiv Sa\|\sim S$	I4,V4,V8,V11,V13
V15	$C\| \equiv D_i\|\sim M_i$	I4, V5,V9
V16	$C\| \equiv pl\|\sim P$	I4, V5,V10

表3给出了协议安全性证明的推理过程。在表3中, 每一行都是根据已有论据来得到某一结论的推理。如表3所示, 为证明V14需要证明V11, V12, V13（V11, V12, V13定义见表3）成立并由I4, V5, V9,V10证明V15, V16成立。

由于对于 h=H(A, B)几乎不可能找到 A1, B1 使得 h=H(A1, B1)故由 V6 得:

$$C \mid\equiv \Phi(M_i, \{M_i\}_{-K_{D_i}}) \quad (V17)$$

$$C \mid\equiv \Phi(P, \{P\}_{-K_{Pl}}) \quad (V18)$$

综上所述, 我们明确了 V14, V15, V16, V1 和 V18 的正确性。因此证明上述溯源协议安全性可以得到保障。

5 TSPPB 防伪溯源系统

5.1 溯源系统设计

基于第 3 节的溯源协议, 本节设计了一个基于区块链技术的防伪溯源系统(Traceability System Using Public and Private Blockchain, TSPPB)。由于直接在公有链中存储每一件产品溯源信息的开销过大(在以太坊中调用智能合约存储一个整数需要花费大约一元), 直接使用区块链来存储溯源信息很难将包括图片文字等格式不同大小不一的溯源信息序列化存储到区块链中。故如图 6 所示, TSPPB 溯源系统使用私有区块链存储溯源验证数据(即溯源数据的哈希值), 同时, 采用 IPFS[11]系统(在本文 5.3 节描述)存储全部的溯源数据, 并在公有区块链中存储私有区块链各区块信息的哈希值。

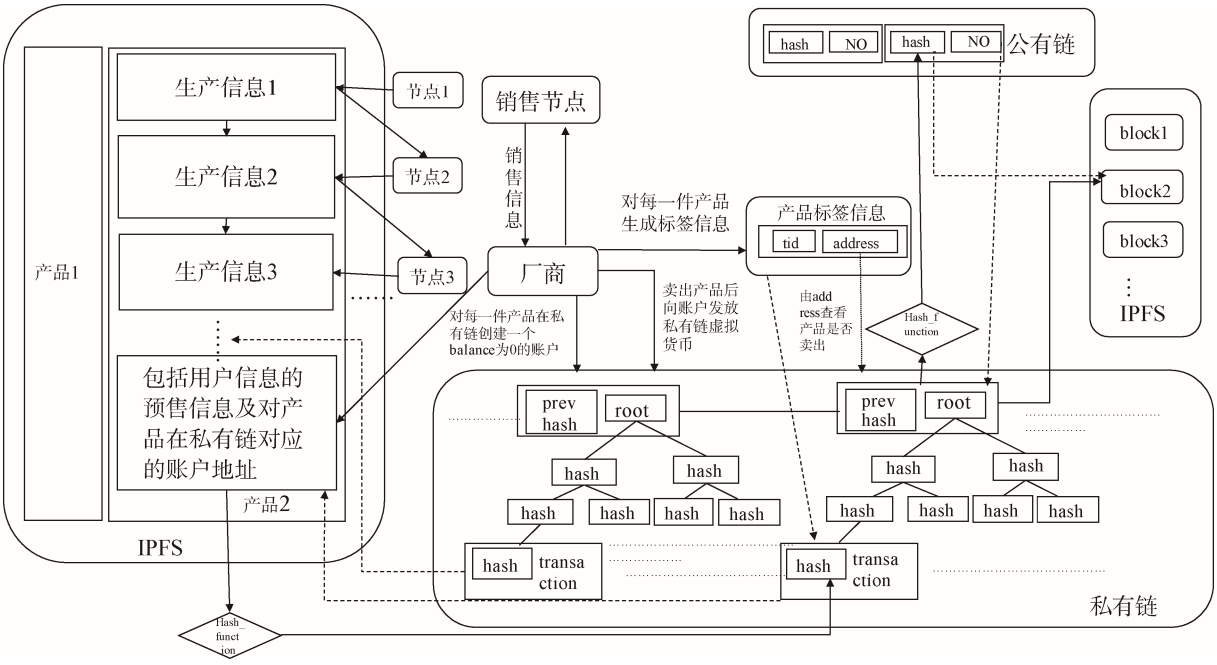


图 6 TSPPB 溯源系统

Figure 6 TSPBB traceability system

5.2 TSPPB 相较传统溯源系统的改进

TSPPB 溯源系统利用区块链的不可篡改的特性来确保溯源信息不被篡改。存储相关溯源信息的同时会存储溯源信息和相关责任人对溯源信息的签名。上述信息及签名的哈希值存储到可靠的区块链系统来保证整个溯源系统中溯源信息的安全性。在第 3 节中, 我们已经证明通过上述方法能够解决责任人绑定的问题。

采用比特币和以太坊区块链等公有链技术的溯源系统却面临着效率低下、信息存储量小、开销高等问题。为解决上述问题, TSPPB 使用如图 6 所示的公有链和私有链一起存储溯源信息。

TSPPB 在私有区块链存储溯源信息的哈希值, 并使用 IPFS 系统存储详细的溯源信息。为保障私有链中存储数据的安全性, TSPPB 将私有链中的数据与以太坊(或比特币)等拥有庞大算力保证的公有区块链进行关联。关联方法可以简略的理解为, 将 TSPPB 的私有链中每个区块所存储数据的哈希值存储到公有链中。

私有链节点可通过查询本地某区块所存储数据的哈希值是否等于公有链中存储的该区块所存储数据正确的哈希值来判断本地区块数据是否被篡改。

厂商对每一件产品在私有区块链中创建一个账户, 并通过操作该账户的 banlance 来防止标签复制, 其原理见 5.5 节。

5.3 溯源记录

图 6 左侧描述了为加入溯源记录的过程。各溯源节点在获得上一溯源节点提供的溯源信息后, 将新的溯源信息及本节点的签名存储到 TSPPB 溯源系统中。

在 TSPPB 溯源系统中, 溯源记录的存储结构如图 7 所示。产品的溯源信息由产品生产加工环节的各节点加入, 各溯源节点需要添加: 溯源信息(溯源信息及产品编号)、该节点对溯源信息的签名(为了

能够追溯产品质量问题的相关责任人, 需要添加相关部门签名)、上一溯源节点所提供信息(包括溯源信息及签名等)的哈希值、溯源信息, 该溯源节点对溯源信息的签名一起做哈希运算得到的哈希值。厂商或溯源节点可通过验证各阶段的溯源信息与签名, 哈希是否匹配验证存储信息是否合法。为方便查询完整的产品的溯源信息, 每一个节点加入的溯源信息还应该包括一个 *transaction_id*, 其作用将在私有区块链与 IPFS 系统中描述 (若为第一个溯源节点加入的溯源信息, 该值为空)。

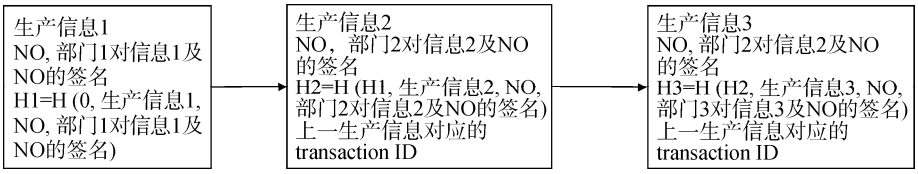


图 7 溯源记录存储结构

Figure 7 Traceability record storage structure

在 TSPPB 溯源系统中, 溯源节点将溯源信息存储到 IPFS 中并将上述信息的哈希通过交易存储到 5.4 节所述的私有区块链系统中。

加入溯源信息的流程如图 8 所示, TSPPB 溯源系统中的某节点(包括物流节点和销售节点)由 tid 获得 *transaction_id*: id1, id1 所指向的交易存储最近加入溯源信息节点所加入的溯源信息的哈希。由该哈希可在 IPFS 系统中获得上述节点所存储的溯源信息。溯源节点加入溯源信息(包括上一生产信息对应的 *transaction_id*)后向溯源系统申请更新产品的 tid 所指向的 *transaction_id* 。新的溯源信息的哈希将存储在一个私有链中的交易里, 令该交易的 *transaction_id* 为 id2。溯源节点提出修改 tid 指向的 *transaction_id* 的申请时, 厂商应该判定该节点所存入信息中上一生产信息对应 *transaction_id* 是否为 tid 当前所指向的 *transaction_id* 以及该节点是否有权限修改 tid, 若上述条件均符合, 则将将 tid 指向 id2。

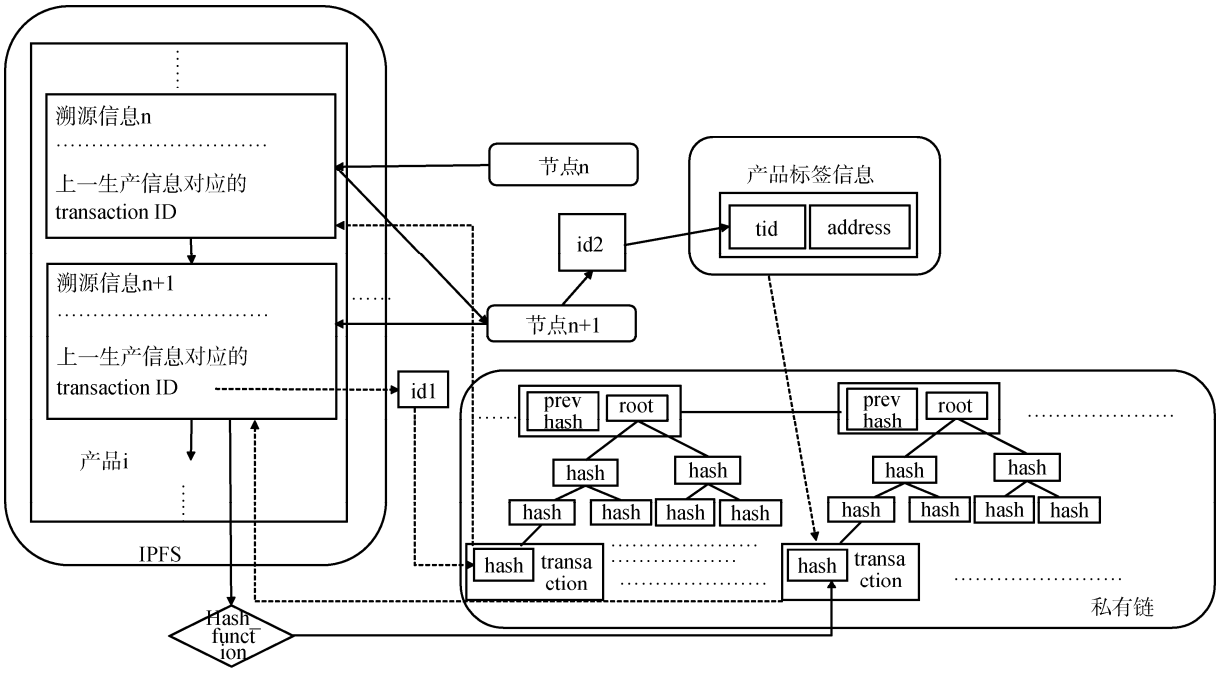


图 8 溯源信息记录过程

Figure 8 The process of traceability information recording

5.4 私有区块链及 IPFS 系统

如图 6 所示, 在 TSPPB 构建一个与 IPFS 相结合的私有区块链系统, 用于存储产品各个生产阶段及销售阶段的信息。详细溯源信息及相关责任人签名将存储在 IPFS 系统中, 而对应的哈希哈希值存储在私链中。

由于 IPFS 系统是内容可寻址的(可通过文件的

哈希找到文件), 故将溯源的完整信息存储到 IPFS 系统中, 完整信息的哈希值存储到私有链中等价于将溯源信息存储私有链中。

如图 9 所示, 为方便查询产品的完整溯源信息, 在 TSPBB 中, 每一个溯源节点加入的溯源信息必须包括一个交易号 *transaction_id* (若为第一个溯源节点该值为空)用于匹配对应的交易。图 9 中的 *transaction_id* 为私有区块链中的某次交易的交易号, 该交易存储了上一溯源节点所记录溯源信息的哈希。因此, 可以根据该哈希值从 IPFS 获得上一溯源信息。

私有链会实现了类似以太坊或比特币的虚拟货币, 账户虚拟货币的余额用 balance 来表示。由于私有链并没有庞大的算力作为支持, 私有链节点间的共识算法可采用 PBFT[12], 或 Dpos 算法。

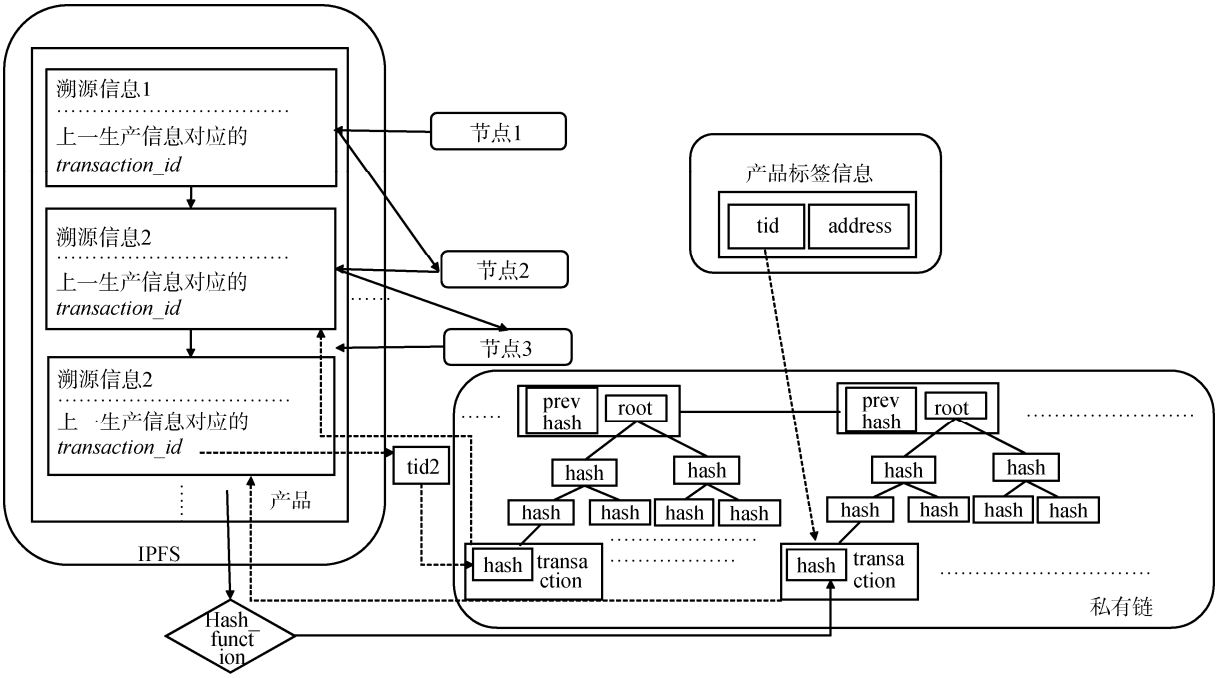


图 9 利用 transaction id 查找上一溯源信息

Figure 9 Find previous traceability information by transaction id

5.5 使用 balance 防止标签复制

在现实生活中, 伪造者可通过复制正品的标签信息欺骗消费者。消费者购买仿冒产品后, 在验证复制的标签信息时能够得到正品的相关信息。为防止此类情况发生, 产品溯源系统需要设计一种手段来防止标签复制行为。TSPPB 采用 TCDBB(tag copy detection based on balance)方式, 利用账户的余额防止标签复制。

在算法 3 中, 使用 p 来表示某件商品, p.account 表示产品在私有区块链的账户, p.account.balance 表示账户 p.account 的 balance 值。Send(account, 1)表示给 account 账户发送值为 1 的 balance(私有链中资金, 没有实际价值)。

算法3. TCDBB算法

输入: 对于每一件产品, 厂商会在私有链中创建一个账户, 并将该账户的信息存储到溯源系统中。

输出: 对于每一件产品, 能够判断该产品是否已经被卖出, 防止标签复制。

过程 3.售卖产品并检查标签复制

```
BEGIN
  If(p.account.banlance!=0)
    return false;
  send(p.account, 1)
  return true;
END
```

对于每一件产品厂商会在私有链创建一个 balance(私有链中资金余额)为 0 的账户并将该账户信息存储到溯源系统中。因为任何人都无法得到商品对应账户的私钥, 故无法使用商品对应账户在私有链中的资金, 即某一产品对应的账户的 balance 只能增加不能减小。若产品对应账户 balance 为 0 说明产品并未卖出。若某产品被卖出, 商家给该产品对应账户汇款(私有链货币, 并没有实际价值), 使下一次使用该标签进行验证时, 产品所对应账户的 balance

不为 0。消费者购买产品前查询产品对应账户的 balance 是否为 0 可得知产品是否已经卖出从而防止标签复制。

5.6 公有区块链及其与私有区块链的关系

与公有区块链相比, 私有链是一种高效、大容量的信息存储方式。但由于私有链拥有的算力有限, 私有区块链系统的安全性并不能得到很好的保障。如图 10 所示, 为保障私有链中存储数据的安全性, TSPPB 将私有链中的数据与等拥有庞大算力的公有区块链进行关联。

多条溯源信息的哈希值被封装在一个区块内, 存储在私有区块链中。TSPPB 溯源系统再将该区块的哈希值存储在公有链中(可通过智能合约)。IPFS 系统中同时存储该区块的备份, 可用于私有链的数据恢复。

溯源过程中, 可对私有链中各区块数据的哈希与公有链中存储的各区块的哈希进行对比检验, 确保私有链中的数据不被篡改。若本地私有链被篡改, 可通过公有链中相关哈希值在 IPFS 系统中获取被篡改区块的原始信息实施私有链的修复。

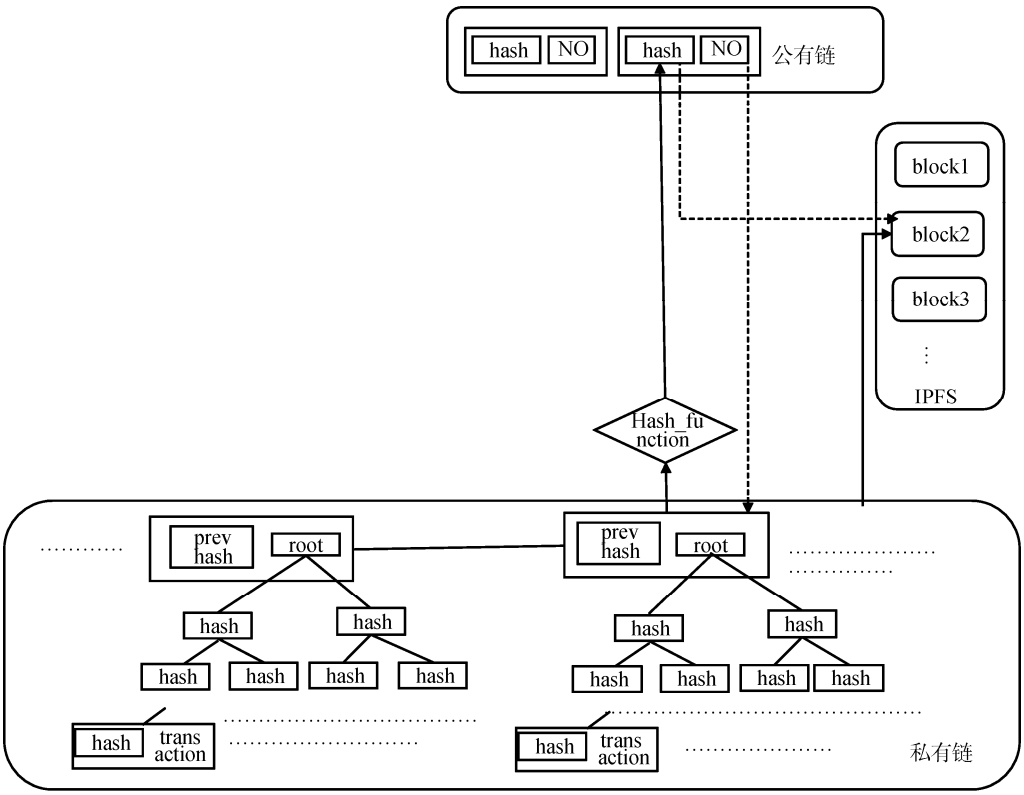


图 10 公有区块链系统与私有区块链系统相结合

Figure 10 The combination of private and public blockchain

5.7 溯源系统运行流程

如图 6 所示, TSPPB 溯源系统中的各个节点将溯源信息按照 5.4 节所述方法添加到私有链及 IPFS 系统中。

厂商对每一件产品生成标签信息, 标签信息包括 tid 以及 address。tid 为指向私有链中记录产品溯源信息最后一个交易的 *transaction_id* 的链接。address 为私有区块链于 IPFS 系统一节中所述的与产品关联的私有链中的账户。

TSPPB 溯源系统按 5.3 节中的方法添加溯源记录。对于每一件产品, 厂商可以向溯源系统添加预售信息。如果商品预售成功, 厂商会将购买人的信息添加到溯源系统中, 如果商品没有被预售, 则厂商会将此信息设为空(或者另外的默认值)。厂商会对每一件商品在私有链创建一个 balance 为 0 的账户并将该账户信息存储到溯源系统中。

用户通过向厂商支付金钱, 预购(或购买)产品。厂商向用户提供产品以及产品的标签信息。

产品卖出后, 商家向该产品对应账户汇款(私有链的货币)。销售产品前若发现该产品对应账户的 balance 不为 0 则说明标签复制。用户购买产品时可查询产品所对应账户的 balance 是否为 0, 如果产品

对应账户的 balance 不为 0 则该产品的标签被复制。

用户在购买产品后可通过 TSPBB 获得产品的溯源信息。用户由 tid 可获得私有链中记录产品溯源信息最后一个交易的 *transaction _id* 。用户可通过下面 gets 算法利用该 *transaction _id* 获得产品的溯源记录最后一个交易的 *transaction _id* 。

算法4. gets()算法

输入: 溯源信息最后一个交易的 *transaction _id*

输出: 产品的溯源信息

过程 4.获得溯源信息

```
BEGIN
  if transaction_id==0) return NULL ;
    h=get_pr(transaction_id);
//get_pr 函数通过一个 transaction_id 可在私有链中获得对应溯源节点所记录的溯源信息哈希 h;
    s=get_s(h);
// get_s()函数可有由前步骤所述的哈希 h 在 IPFS 系统中获得 h 对应的详细溯源信息
    id=get_id(s);
// get_id()函数通过 s 获得指向上一溯源节点所记录信息的哈希值的 transaction _id 。
    return s+gets(id);// 递归调用本函数
END
```

6 溯源协议测试

本节将对第三节的溯源系统进行性能分析。在本文的实现中, 通过调用合约实现公有链的功能, 并测试系统的公有链智能合约功能。搭建了以太坊私有链存储详细溯源信息。并通过创建一个以太坊的创世块文件, 构建以太坊私有链。私有链搭建后, 使用 geth 客户端在局域网内部署 2 个私有链节点。

在实验中, 完整的溯源信息和相关智能合约分别存储和部署到以太坊私有链中, 溯源信息的哈希值存储到以太坊公有链下, 用于测试溯源系统私有链部分的响应时间.

部署在私有链的合约实现了以下功能:

1. 向私有链中加入生产计划或某一生产步骤的生产信息。(在实验中定义为: 添加者、添加时间和一个 string)

2. 添加销售信息。(在实验中定义为: 三个 string 用于记录销售地点、商家和时间)

3. 由标签信息获得私有链中各个生产流程及生产计划(在实验中定义了 3 个流程)的信息。

在实验中, 实现了上述功能的 web3.js 的合约接口, web 页面可以通过这些接口调用实现上述功能的函数。网页响应及合约运行时间的总和如图 11 所示。

在第 1 个功能点中, 因为以太坊通过交易来调用合约, 交易都需要发起者签名。因此添加者信息采用信息者的签名即可。第 2 功能点中, 合约规定了添加溯源信息特定条件(本实验设定符合某特定地址才能添加销售信息)。

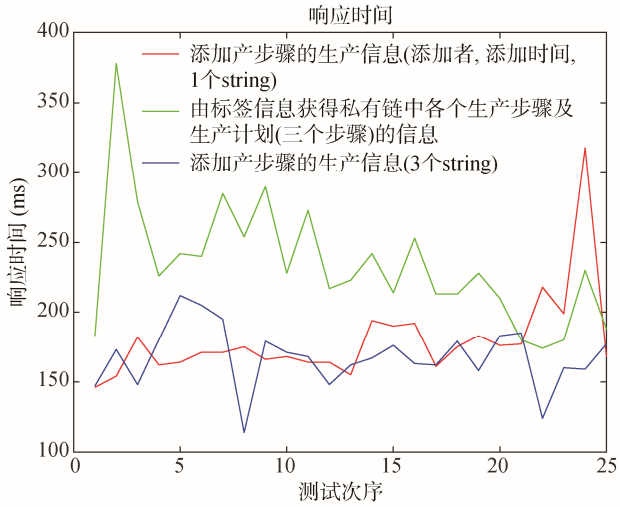


图 11 响应时间

Figure 11 Response time

如图 11 所示, 对于在私有链中实现的功能, 本文对其进行了 25 次测试。向私有链中加入生产计划或某一生产步骤的生产信息, 花费时间在 146ms 到 318ms 之间, 添加销售信息花费时间在 114ms 到 212ms 之间, 由标签信息获得私有链中各个生产步骤及生产计划的信息花费时间在 174ms 到 378ms 之间。

由于私有链的节点使用局域网相连, 其网络时延迟远小于以太坊公有链, 且在私有链中交易很少, 调用合约的交易会马上被挖矿节点接受, 故私有链的响应时间与公有链的响应时间相比可以忽略不计。相较于其它非挖矿节点, 这些节点可以在一个区块时间(可自己按需求设定)后获得对区块链做出操作的交易信息。

实验通过以太坊的智能合约来实现公有链的功能。智能合约的调用需要通过交易实现, 交易生效过程需要消耗 gas, gas price 即为交易支付的实际费用。对于公有链部分, 若使用智能合约来实现第 3 节所描述的协议, 在以太坊智能合约中存储的产品标签(产品信息的哈希值、消费信息及私有链中存储信息的链接)的基本花费为 635917gas。设 gas price 为 1 Gwei, 则交易花费 0.00064 个以太币。设以太币的价

格为 1045 美元, 每存储一个产品的溯源信息都将花费 0.665 美元。

为节省开支, 如果在公有链中只存储私有链中每个区块对应的哈希值, 并使用智能合约来实现上述功能, 则存储私有链中一个区块需要花费 47509 gas。此时, 将一个私有区块的哈希值存储到公有链, 需花费 0.05 美元, 若一个区块中存储 10000 件产品的信息, 则每件产品存储到溯源系统的成本为 0.000005 美元。

若直接在以太坊中存储每一步的溯源信息(在本实验中为一个 string), 存储每一步溯源信息将花费 84884gas。此时, 在以太坊中调用合约的开销为: $gas\_\cos t \times gas\_price$, 若溯源系统中的产品需要存储 n 各步骤的溯源信息, 则总开销为:

$$n \times gas\_\cos t \times gas\_price \tag{V19}$$

以太坊公有链中每存储一件产品的溯源信息的开销与记录产品溯源信息步骤数的关系如表 4 所示。

通过表 4, 若一件产品的溯源信息需要通过 20 步来存储, 则在以太坊公有链中每存储一件产品需要花费 1.76 美元。

表 5 分析了三种存储方式, 即在公有链存储每件产品的标签信息、公有链中存储私有链中一个区块信息的哈希值和公有链中直接存储溯源信息(20 步)的开销对比。通过表 5 我们可以看到, 在公有链中存储私有链中一个区块信息的哈希相较与在公有链中存储每件产品的标签信息或直接存储溯源信息将极大的节省开支。

表 4 在以太坊公有链中存储溯源信息开销

Table 4 The overhead of traceability information storage using ethereum

步数	开销(美元)
10	0.88
20	1.76
30	2.64
40	3.52

表 5 存储一件产品溯源信息成本开销

Table 5 The overhead of traceability information storage per product

公有链存储每件产品的标签信息(美元)	公有链中存储私有链中一个区块信息的哈希(美元)	公有链中直接存储溯源信息(美元)
0.665	0.000005	1.76

在本实验中, 公有链系统的响应时间主要由调用合约的交易生效的时间影响。在以太坊中调用合约的速度与交易的 gas price(支付给旷工的报酬)有关。图 12 描述了区块号为 4916230 的区块(实验时为最新的区块)中交易生效的时间与 gas price 的关系。可以看到, gas price 越高(支付给旷工的报酬越多), 交易生效越快, 即公有链系统的响应速度越快。

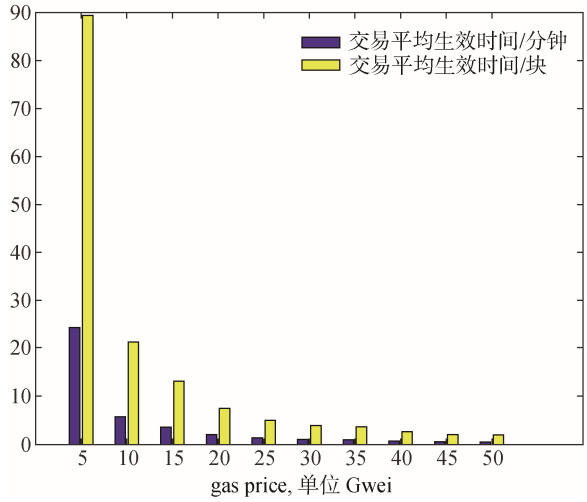


图 12 交易生效的时间与 gas price 的关系

Figure 12 The relationship between the time required for the transaction to be acceptedand gas price

7 结论与展望

本文提出了一种基于双区块链技术的溯源系统 TSPPB, 相较与传统的产品溯源系统, 借助于区块链不可篡改与可溯的特性, 该溯源系统拥有以下优势:

1. 能够基于区块链的不可篡改的特性, 防止产品信息的篡改。

2. 利用区块链中的账户余额, 设计了对应协议, 防止正品的标签信息被赝品复制。

3. 提出了相关算法, 当产品如果出现质量问题时, 能够快速定位相关责任人。

4. 设计的系统, 能够有效防止生产方超出应有产量随意滥发产品。

为减少溯源协议的运行成本, 我们将该溯源协议所使用的区块链分为公有链和私有链两个部分, 并提出了采用IPFS进行复杂信息的存储方式。利用私有链能够高效、大容量的存取信息的优势和公有区块链可信度高的特点将两种方式相结合, 设计了一种实用的溯源系统, 并在上述基础上完成了3种溯源模式的性能和开销的分析。后续还会做更深入的研究, 例如构建更安全和响应速度更快, 更为方便部署的私有链系统, 能够提供更多方位的认证模式和交互接口等。

本文对区块链技术和智能合约技术在溯源应用领域中有益的研究探索，虽然这些技术目前还面临很多问题和挑战，但相信这些技术能够在数字社会中起到关键作用。

参考文献

[1] Sheng Mingyan, “Research on the Traceability of Cold Chain Logistics Information of Fruit and Vegetable Agricultural Products,” Suzhou University of Science and Technology, 2017.

[2] Abeyratne, Saveen A., and Radmehr P. Monfared., “Blockchain ready manufacturing supply chain using distributed ledger ,” International Journal of Research in Engineering and Technology, pp. 1-10,September 2016.

[3] Regattieri, A, Gamberi, M, and Manzini, “Traceability of food products: General framework and experimental evidence,”. Journal of food engineering 81 pp. 347-356 2007.

[4] “Eximchain: Supply Chain Finance solutions on a secured public, permissioned blockchain hybrid, ” https://eximchain.com/ Whitepaper%20-%20Eximchain.pdf, March. 2018.

[5] Tian, Feng, “An agri-food supply chain traceability system for China based on RFID & blockchain technology, ,” IEEE International Conference on Service Systems and Service Management(ICSSSM).,January 2016.

[6] Feng T, “A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things, ” IEEE International Conference on Service Systems and Service Management (ICSSSM)., January 2017.

[7] “Waltonchain White Paper,” https://www.waltonchain.org/ templets-/default/doc/Waltonchain-whitepaper_en_20180208.pdf, February 2018.

[8] Becker G, “Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis[J],” 2013.

[9] Zhu Yan, and Gan Guohua, “Blockchain Safety Technology: Status Quo, Problems and Progress,” http://www.sohu.com/a/141183400_61-0499, May. 2017.
朱岩，甘国华，“区块链安全技术：现状、问题与进展”, http://www.sohu.com/a/141183400_610499, 2017) .

[10] Karame G, “On the Security and Scalability of Bitcoin's Blockchain[C],” ACM Sigsac Conference on Computer and Communications Security, pp. 1861-1862, 2016.

[11] Benet, and Juan, “IPFS - Content Addressed, Versioned, P2P File System,” Eprint Arxiv , 2014.

[12] Bentov I, Gabizon A, and Mizrahi A, “Cryptocurrencies Without Proof of Work[J],” Computer Science, pp. 142-157, 2014.

[13] Cohen B, “Incentives Build Robustness in BitTorrent[J],” Proc P Economics Workshop, 2003.

[14] Andrychowicz M, Dziembowski S, and Malinowski D, “Secure multiparty computations on Bitcoin[C],” IEEE Security and Privacy, pp. 76-84, 2014.

[15] Andrychowicz M, Dziembowski S, and Malinowski D, “Fair Two-Party Computations via Bitcoin Deposits[M],” Financial Cryptography and Data Security, pp. 105-121, 2014.

[16] Ha J C, Kim H K, and Park J H, “HGLAP – Hierarchical Group-Index Based Lightweight Authentication Protocol for Distributed RFID System[M],” Springer Berlin Heidelberg Emerging Directions in Embedded and Ubiquitous Computing, pp. 557-567, 2007.

[17] “Bitcoin developer reference,” https://hitcoin.org/en/developer-referen-ce#get-tx, 2009.

[18] Richard Brown, “A Simple Model for Smart Contracts,” https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts, Dec. 2014.

[19] Florian Glatz, “What are Smart Contracts,” https://medium.com/@hec-kerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad, Dec. 2014.

[20] Luu L, Chu D H, and Olickel H, “Making smart contracts smarter[C],” Proceedings of the 2016 ACM Conference on Computer and Communications Security(SIGSAC), pp. 254-269, 2016.

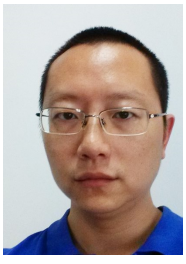
[21] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella, “Fairplay - a secure two-party computation system,” In Proceedings of the 13th Conference on Security Symposium (USENIX), pp. 20-20, 2004.

[22] Assaf Ben-David, Noam Nisan, and Benny Pinkas, “Fairplay MP: a system for secure multi-party computation,” In Proceedings of the15th Conference on Computer and Communications Security(CCS), pp. 257-266, October. 2008.

[23] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,”2008.

[24] “Analysis of the DAO exploit,” http://hackingdistributed.com/-2016/0618/analysis-of-the-dao-exploit, June. 2016.

刘家稷 于2016年在电子科技大学生物医学工程专业获得学士学位。现于电子科技大学计算机科学与技术专业攻读硕士学位。研究领域为区块链技术。研究兴趣包括：机器学习、自组织网络。Email: 1925074700@qq.com



杨挺 于2014年在电子科技大学获得博士学位，现任电子科技大学计算机科学与工程学院软件工程研究中心讲师，研究领域为计算机网络，研究兴趣包括：自组织网络、区块链技术、物联网技术。Email: yting@uestc.edu.cn