



(12) 发明专利

(10) 授权公告号 CN 109886675 B

(45) 授权公告日 2021. 03. 30

(21) 申请号 201910104337.X

H04L 29/08 (2006.01)

(22) 申请日 2019.02.01

(56) 对比文件

(65) 同一申请的已公布的文献号
申请公布号 CN 109886675 A

CN 108694575 A, 2018.10.23

CN 108923908 A, 2018.11.30

CN 108614974 A, 2018.10.02

(43) 申请公布日 2019.06.14

CN 108810006 A, 2018.11.13

CN 107682331 A, 2018.02.09

(73) 专利权人 杭州电子科技大学
地址 310018 浙江省杭州市下沙高教园区2号大街

CN 108965299 A, 2018.12.07

US 2019026450 A1, 2019.01.24

US 2018367314 A1, 2018.12.20

(72) 发明人 吕秋云 祁伊祯 郑宁

董贵山等. 基于区块链的身份管理认证研究. 《计算机科学》. 2018, 第52-59页.

(74) 专利代理机构 杭州君度专利代理事务所
(特殊普通合伙) 33240

审查员 李慧芳

代理人 朱月芬

(51) Int. Cl.

G06Q 20/36 (2012.01)

G06Q 20/38 (2012.01)

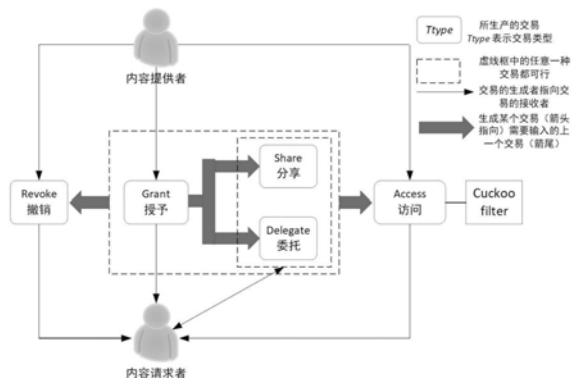
权利要求书2页 说明书8页 附图3页

(54) 发明名称

基于区块链的资源访问令牌的分发和资源使用监控方法

(57) 摘要

本发明公开了一种基于区块链的资源访问令牌的分发和资源使用监控方法。本发明通过区块链交易的形式实现访问令牌的安全分发和资源使用的有效监控。内容提供者以访问令牌授予交易的形式将访问令牌授予内容请求者，如果内容请求者拥有该访问令牌的分享权限或者委托权限，说明该访问令牌可以被内容请求者分享给其他用户或者委托给第三方。内容请求者使用所获得的访问令牌访问内容，对应的内容访问操作将以内容访问交易的形式被记录在区块链上。本发明还通过令牌撤销交易实现访问令牌的撤销，以增强了访问控制的安全性。本发明提高了访问令牌的验证效率，从而提高整个系统的访问效率。



1. 基于区块链的资源访问令牌的分发和资源使用监控方法,其特征在于包括设置访问交易格式、访问令牌的安全分发、访问令牌的撤销、内容访问的监控以及使用Cuckoo filter的快速检索;

所述的设置访问交易格式,具体实现如下:

分发访问令牌AccToken的访问交易 T_{Type} 定义为:

$$T_{Type} = (Tid, Ttype, Tin[PK_i, T_{pre}, \varphi], Tout[PK_j, AccToken, \varpi]) \quad (1)$$

在式子(1)中, Tid表示交易标识; Ttype表示交易类型; Tin[]为交易输入数组包括交易创建者的地址 PK_i 、访问令牌AccToken的上一次交易 T_{pre} 以及交易输入脚本 φ ; Tout[]表示交易输出数组包括交易输出地址 PK_j 、被交易的访问令牌AccToken和交易输出脚本 ϖ ;

访问令牌的安全分发,根据不同的访问需求设计有3种访问令牌的分发方式,并以区块链交易的形式进行访问令牌分发,分别为:访问令牌的授予Grant交易、访问令牌分享Share的交易和访问令牌的委托Delegate交易,具体实现如下:

2-1 访问令牌的授予交易

当内容提供者第一次响应内容请求者的访问请求时,内容提供者将访问令牌以访问令牌授予交易 T_{Grant} 的形式分发给内容请求者,其中 T_{Grant} 如下所示:

$$T_{Grant} = (Tid, Grant, Tin[PK_{cp}, \phi, \phi], Tout[PK_{CQ}, AccToken_g, \varpi]) \quad (2)$$

在式子(2)中, T_{Grant} 是访问令牌AccToken的初始交易,因而它的 T_{pre} 和 φ 都为空,可以记作 ϕ ; T_{Grant} 用于访问令牌的授予,所以它的访问类型为Grant;

2-2 访问令牌的分享交易

当内容请求者B通过访问令牌授予交易从内容提供者A获取访问令牌之后,内容请求者B拥有访问令牌的分享权限, B还可以将该访问令牌分享给其他请求者,此时内容请求者B也被称为分享者B;而分享者B能够通过访问令牌的分享交易 T_{share} 将访问令牌分享给请求者C,分享交易 T_{share} 如下所示:

$$T_{share} = (Tid, Share, Tin[PK_B, T_{pre}, \varphi], Tout[PK_C, AccToken, \varpi]) \quad (3)$$

在式子(3)中, T_{pre} 是内容提供者A授予分享者B的访问令牌授予交易 T_{Grant} , PK_B , PK_C 分别表示分享者B和请求者C的地址;

2-3 访问令牌的委托交易

访问令牌的委托交易用于处理当内容提供者A需要将该访问令牌通过该内容请求者D委托给第三方C的情况,而此时内容请求者D也被称为委托者D;此过程首先内容提供者A通过令牌授予交易 T_{Grant} 将访问令牌分发给委托者D,然后委托者D生成访问令牌的委托交易 $T_{delegate}$,通过 $T_{delegate}$ 将访问令牌委托给第三方C, $T_{delegate}$ 如下所示:

$$T_{delegate} = (Tid, Delegate, Tin[PK_D, T_{pre}, \varphi], Tout[PK_C, AccToken, \varpi]) \quad (4)$$

在式子(4)中, T_{pre} 是内容提供者A授予委托者D的访问令牌授予交易 T_{Grant} , PK_D , PK_C 分别表示委托者D和请求者C的地址;注意:委托者D有且只有一次可以把内容委托给第三方;

访问令牌的撤销,具体实现如下:

访问令牌的撤销分两种情况:

一是访问令牌的过期失效;

二是在有效期内,访问令牌的创建者主动撤销访问令牌;

对于情况一:任何访问令牌的验证者都可以对已过期的访问令牌进行撤销;

对于情况二:如果用户想要撤销由他自己授予、分享或委托的访问令牌,他可以生成访问令牌撤销交易 T_{revoke} ,如下所示:

$$T_{revoke} = (Tid, Revoke, Tin[PK_{user}, T_{pre}, \phi], Tout[\phi, AccToken, \phi]) \quad (5)$$

在式子(5)中, T_{pre} 表示该访问令牌上一次的交易, PK_{user} 表示启动该访问令牌撤销的用户的地址,输出地址和输出交易都设置为空,从而确保已撤销的访问令牌不再在区块链上传输;

内容访问的监控,具体实现如下:

内容请求者B使用已签名的访问令牌向内容提供者A发送请求以访问内容,内容提供者A先验证内容请求者B的访问令牌,之后为B提供内容同时A将生成内容访问交易 T_{access} ,见式子(6);访问令牌的验证过程如下所示:

(1) 令牌签名验证:A使用内容请求者B的公钥进行签名验证,若验证失败拒绝访问,否则继续验证;

(2) 时间验证:A验证访问令牌是否已过期,若是拒绝访问,否则继续验证;

(3) 撤销验证:A在区块链上检索该访问令牌的撤销交易,若存在说明该访问令牌已被撤销,拒绝访问,否则继续验证;

(4) 授予验证:A在区块链上检索该访问令牌的授予交易,若存在说明该访问令牌是合法令牌,可以为内容请求者B提供内容;

如果内容请求者B通过以上的验证,A将为B提供访问内容之后将生成一个关于B使用该访问令牌的内容访问交易 T_{access} ;

$$T_{access} = (Tid, Access, Tin[PK_A, T_{pre}, \phi], Tout[PK_B, AccToken || access, \varpi]) \quad (6)$$

在本方法中,涉及访问令牌的所有操作都以交易的形式记录在区块链上,包括访问令牌的分发,使用访问令牌的内容访问操作以及访问令牌的撤销,这将组成一个全面的内容提供者的资源使用监控;输出数组 $Tout[]$ 中的 $AccToken || access$ 表示所使用的访问令牌和对应的内容;

使用Cuckoo filter的快速交易检索,具体实现如下:

分别为已授予的访问令牌和已撤销的访问令牌构建Cuckoo filter,分别记作 CF_g , CF_{inv} ;当矿工验证一个访问令牌授予交易成功后,矿工将该令牌的哈希 $H(AccToken)$ 添加到 CF_g 同时将该交易写入区块链;而当矿工验证一个访问令牌撤销交易成功后,他只需从 CF_g 中删除 $H(AccToken)$ 并将 $H(AccToken)$ 添加到 CF_{inv} 同时将该交易写入区块链;用户无需再检索整个区块链以实现访问令牌的有效性验证,只需查询 CF_g , CF_{inv} 就可实现。

基于区块链的资源访问令牌的分发和资源使用监控方法

技术领域

[0001] 本发明涉及区块链、访问控制和访问令牌技术领域，具体涉及一种基于区块链的资源访问令牌的分发和资源使用监控方法。

背景技术

[0002] 访问令牌最初是Windows操作系统安全性的一个概念。当用户登陆时，系统创建一个访问令牌，该令牌包含了用户登录进程时返回的SID和由本地安全策略分发给用户和用户的安全组的特权列表。系统使用令牌控制用户可以访问哪些安全对象，但是它仅适用于本地登陆访问。而在目前使用访问令牌的访问控制方案中，都将访问令牌作为一个凭证从而进行内容的远程访问，但这些带令牌的访问控制方案中普遍存在以下问题：

[0003] (1) 访问令牌传输的安全和隐私问题。当前访问控制方案中，访问令牌要么直接传输，要么加密传输，这都将带来访问令牌的安全和隐私问题，如果直接传输那么该令牌很容易被伪造，冒用等，而加密传输虽然无法知道令牌的具体内容，但是通过抓包很容易泄露使用者的身份隐私。

[0004] (2) 存在访问令牌撤销难问题。传统的方案中，往往对应访问令牌的撤销问题考虑欠缺，要么完全撤销，这将会带来巨大的计算和通信开销，要么部分撤销，这使得之前的访问令牌依然可以进行正常的内容访问。

[0005] (3) 未考虑资源使用监控。当前的相关方案中，一旦内容提供者授予了内容请求者访问令牌(访问权限)，内容请求者将任意使用该资源，且内容提供者无法知晓内容请求者对于资源的具体使用情况。这容易导致资源的被私自泄露和滥用，且即使知道资源被泄露或者滥用了内容提供者也很难追责。

[0006] 随着互联网的发展，区块链技术受到广泛关注。而区块链的防篡改性、匿名性以及去中心化等特性，可以很好的解决以上几个问题，但是在区块链中，每次查询记录在区块链上的某个内容，都必须遍历整个区块链，随着区块链的增加，它的将带来大量的计算开销。

发明内容

[0007] 本发明主要针对目前存在的使用访问令牌进行访问控制的方案中的不足，提供一种基于区块链的资源访问令牌分发和资源使用监控方法。

[0008] 本发明包括访问交易格式、访问令牌的安全分发、访问令牌的撤销、内容访问的监控以及使用Cuckoo filter的快速检索。本发明基于区块链交易实现访问令牌安全分发和资源使用的有效监控，可以适用于任何使用访问令牌(或访问凭证)的访问控制系统，其结构如图1所示，具体实现过程如下：

[0009] 步骤1、设置访问交易格式

[0010] 在区块链中，每个交易都由三部分组成：交易标识(Tid)、交易的输入数组Tin[]和交易的输出数组Tout[]。而在本发明中，我们增加了一个新的字段：交易类型(Ttype)，以便于快速查找某一交易记录而无需遍历整个区块链，而其中交易类型包括授予(Grant)、分

享 (Share)、委托 (Delegate)、撤销 (Revoke) 和访问 (Access), 可表示为 $T_{type} \in \{Grant, Share, Delegate, Revoke, Access\}$ 。因此, 本发明中访问交易 T_{Type} 的交易格式用公式表示如公式 (1) 所示:

$$[0011] \quad T_{Type} = (Tid, Ttype, Tin[PK_i, T_{pre}, \phi], Tout[PK_j, AccToken, \varpi]) \quad (1)$$

[0012] 在公式 (1) 中, PK_i, PK_j 分别表示交易的创建者和接收者地址; T_{pre} 表示访问令牌 (AccToken) 的上一次交易; ϕ 是一个输入脚本, 用于获取之前交易的访问令牌; ϖ 是一个输出脚本, 给出获取交易 T_{Type} 中所分发的访问令牌的条件。为了更加清晰的阐述, 本发明的访问交易格式也可如表1所示。

[0013] 表1访问交易 T_{Type}

$T_{Type} \text{ (in: } T_{pre} \text{)}$	
交易类型:	$Ttype$
访问令牌:	$AccToken$
输入脚本 ϕ:	$\phi \text{ or } Sig_{sk_{cp}}(T_{pre})$
输出脚本 ϖ ($body, \sigma$):	$Ver_{PK_{CQ}}(body, \sigma)$

[0014] 在表1中, $body$ 包括 $T_{pre}, Ttype, AccToken, PK_{CQ}$; σ 表示内容提供者对该访问交易的签名。如果该访问交易是一个初始交易, 那么它的输入交易为空, 可用 ϕ 表示。

[0015] 步骤2访问令牌的安全分发

[0016] 本发明根据不同的访问需求设计了3种访问令牌的分发方式, 并以区块链交易的形式进行访问令牌分发, 分别为: 访问令牌的授予 (Grant) 交易、访问令牌分享 (Share) 的交易和访问令牌的委托 (Delegate) 交易。

[0017] 2-1访问令牌的授予 (Grant) 交易

[0018] 当内容提供者第一次响应内容请求者的访问请求时, 内容提供者将访问令牌以授予访问令牌交易的方式分发给内容请求者, 访问令牌的授予的详细过程如图2所示, 具体过程如下:

[0019] (1) 内容请求者通过网络发送访问请求 (可以带一些身份标识数据, 具体根据所用的访问控制模型)。

[0020] (2) 内容提供者接收该请求, 身份认证通过之后为该请求者生成访问令牌。

[0021] (3) 内容提供者根据该访问令牌生成访问令牌的授予交易 T_{Grant} 如下所示:

$$[0022] \quad T_{Grant} = (Tid, Grant, Tin[PK_{cp}, \phi, \phi], Tout[PK_{CQ}, AccToken_g, \varpi]) \quad (2)$$

[0023] 在式子 (2) 中, T_{Grant} 是访问令牌 $AccToken$ 的初始交易, 因而它的 T_{pre} 和 ϕ 都为空, 可以记作 ϕ 。 T_{Grant} 用于访问令牌的授予, 所以它的访问类型为 $Grant$ 。

[0024] (4) 该访问令牌的授予交易将被广播到区块链中。

[0025] (5) 矿工根据共识协议验证交易的有效性, 若有效则写入区块链中转入到步骤 (7), 否则拒绝进行步骤 (6)。

[0026] (6) 若交易被拒绝, 将会通知内容请求者, 内容请求者可再次发送请求。

[0028] (7) 内容请求者使用自身的私钥SK_{CQ}从区块链中获取访问令牌。

[0029] 而访问令牌的分享 (Share) 交易和委托 (Delegate) 交易中, 交易的广播和矿工验证方式以及访问令牌的获取方式和1-2相同, 将不再赘述。

[0030] 2-2访问令牌的分享 (Share) 交易

[0031] 当内容请求者B通过访问令牌授予交易从内容提供者A获取访问令牌之后, 如果内容请求者B拥有访问令牌的分享权限, B还可以将该访问令牌分享给其他请求者 (例如请求者C), 此时内容请求者B也被称为分享者B, 如图3所示。而分享者B可以通过访问令牌的分享交易T_{share}将访问令牌分享给请求者C, 分享交易T_{share}如下所示:

$$[0032] \quad T_{share} = (Tid, Share, Tin[PK_B, T_{pre}, \phi], Tout[PK_C, AccToken, \varpi]) \quad (3)$$

[0033] 在式子 (3) 中, T_{pre}是内容提供者A授予分享者B的访问令牌授予交易T_{Grant}, PK_B, PK_C分别表示分享者B和请求者C的地址。

[0034] 2-3访问令牌的委托 (Delegate) 交易

[0035] 访问令牌的委托交易用于处理当内容提供者A需要将该访问令牌通过该内容请求者D委托给第三方请求者C的情况, 而此时内容请求者D也被称为委托者D, 如图4所示。此过程首先内容提供者A通过令牌授予交易T_{Grant}将访问令牌分发给委托者D, 然后委托者D生成访问令牌的委托交易T_{delegate}, 通过T_{delegate}将访问令牌委托给第三方请求者C, T_{delegate}如下所示:

$$[0036] \quad T_{delegate} = (Tid, Delegate, Tin[PK_D, T_{pre}, \phi], Tout[PK_C, AccToken, \varpi]) \quad (4)$$

[0037] 在式子 (4) 中, T_{pre}是内容提供者A授予委托者D的访问令牌授予交易T_{Grant}, PK_D, PK_C分别表示委托者D和第三方请求者C的地址。注意: 委托者D有且只有一次可以把内容委托给第三方请求者C。

[0038] 步骤3访问令牌的撤销

[0039] 访问令牌的撤销可以分为两种情况: 一是访问令牌的过期失效; 二是在有效期内访问令牌的创建者主动撤销访问令牌。对于情况一: 任何访问令牌的验证者都可以对已过期的访问令牌进行撤销; 对于情况二: 如果某一用户想要撤销由他自己授予、分享或委托的访问令牌, 他可以生成访问令牌撤销交易T_{revoke}, 如下所示:

$$[0040] \quad T_{revoke} = (Tid, Revoke, Tin[PK_{user}, T_{pre}, \phi], Tout[\phi, AccToken, \phi]) \quad (5)$$

[0041] 在式子 (5) 中, T_{pre}表示该访问令牌上一次的交易, PK_{user}表示启动该访问令牌撤销的用户的地址, 输出地址和输出交易都设置为空 (可以 ϕ 表示) 是为了确保已撤销的访问令牌不再在区块链上传输。

[0042] 步骤4内容访问的监控

[0043] 内容请求者B使用已签名的访问令牌AccToken || σ 向内容提供者A发送请求以访问内容, 内容提供者A先验证内容请求者B的访问令牌, 之后为B提供内容同时A将生成内容访问交易T_{access}, 如图5所示。访问令牌的验证过程 (见图6) 具体步骤如下所示:

[0044] 4-1. 令牌签名验证, A使用内容请求者B的公钥进行签名验证, 若验证失败拒绝访问, 否则继续验证。

[0045] 4-2. 时间验证, A验证访问令牌是否已过期, 若是拒绝访问, 否则继续验证。

[0046] 4-3. 撤销验证, A在区块链上检索该访问令牌的撤销交易, 若存在说明该访问令牌

已被撤销,拒绝访问,否则继续验证。

[0047] 4-4. 授予验证,A在区块链上检索该访问令牌的授予交易,若存在说明该访问令牌是合法令牌,可以为内容请求者B提供内容。

[0048] 如果内容请求者B通过以上的验证,A将为B提供访问内容之后将生成一个关于B使用该访问令牌的内容访问交易 T_{access} ,如下所示:

$$[0049] \quad T_{access} = (Tid, Access, Tin[PK_A, T_{pre}, \varphi], Tout[PK_B, AccToken || access, \varpi]) \quad (6)$$

[0050] 在式子(6)中, T_{pre} 表示该访问令牌上一次的交易,输出数组 $Tout[]$ 中的 $AccToken || access$ 表示所使用的访问令牌和对应的内容访问操作。

[0051] 在本发明中,涉及访问令牌的所有操作都以交易的形式记录在区块链上。这些操作包括访问令牌的分发(授予、分享和委托),使用访问令牌的内容访问操作以及访问令牌的撤销,这将组成一个全面的内容提供者的资源使用监控。内容提供者想要追责或者查询自己内容的访问情况都可以通过查找区块链获取,而区块链的防篡改特性也保证了资源使用监控的正确性。

[0052] 步骤5使用Cuckoo filter的快速交易检索

[0053] 为了提高区块链中交易记录的检索效率,本发明引入了Cuckoo filter。Cuckoo filter是一种高效的数据结构,支持动态添加和删除条目比Bloom filter拥有更好的检索性能和更少的空间使用率。一个Cuckoo filter由多个桶组成,而其中一个桶可以由多个实体,而每个实体存储一个指纹。对于添加条目 x ,先使用哈希函数计算两个候选桶 b_1 和 b_2 的索引如下所示(其中 $fingerpr\ int(x)$ 是 $hash(x)$ 的最低 k bits, M 表示桶的数量):

$$[0054] \quad \begin{aligned} b_1 &= hash(x) \bmod M \\ b_2 &= b_1 \oplus hash(fingerprint(x)) \bmod M \end{aligned} \quad (7)$$

[0055] 如果候选桶中有空桶,将 $fingerpr\ int(x)$ 保存到空桶中,否则,只需选择一个候选存储桶,删除它现有的条目,然后将此条目重新插入其候选桶中,重复该过程直到找到空桶或超过最大位移数。在Cuckoofilter中的查找过程是先给定条目 x ,然后根据式子(7)计算 $fingerpr\ int(x)$ 和两个候选桶,最后遍历两个候选桶,如果任一桶中的任何现有指纹匹配,返回true,否则返回false。在Cuckoo filter中删除条目过程为,先检查给定项 x 的两个候选桶,如果 $fingerpr\ int(x)$ 匹配任意一个候选桶中的条目,从该桶中删除该匹配 $fingerpr\ int(x)$ 的一个副本。

[0056] 在本发明中,我们分别为已授予的访问令牌和已撤销的访问令牌构建Cuckoo filter,分别记作 CF_g, CF_{inv} 。当矿工验证一个访问令牌授予交易成功后,他将该令牌的哈希 $H(AccToken)$ 添加到 CF_g 同时将该交易写入区块链;而当矿工验证一个访问令牌撤销交易成功后,他只需从 CF_g 中删除 $H(AccToken)$ 并将 $H(AccToken)$ 添加到 CF_{inv} 同时将该交易写入区块链。这将提高用户在访问令牌验证过程的验证效率,用户无需再检索整个区块链以实现访问令牌的有效性验证,只需查询 CF_g, CF_{inv} 就可实现。

[0057] 本发明有益效果如下:

[0058] 本发明提高用户在访问令牌验证过程的验证效率,用户无需再检索整个区块链以实现访问令牌的有效性验证,只需查询 CF_g, CF_{inv} 就可实现。

[0059] 本发明基于区块链,交易实现访问令牌安全分发和资源使用的有效监控,可以适用于任何使用访问令牌(或访问凭证)的访问控制系统。

[0060] 发明通过令牌撤销 (Revoke) 交易实现访问令牌的撤销,以增强了访问控制的安全性。

[0061] 本发明引入了Cuckoo filter提高了访问令牌的验证效率,从而提高整个系统的访问效率。

[0062] 综上所述,在本发明中,访问令牌的分发、使用以及撤销都以交易的形式记录在区块链上,这将形成一个全面的资源使用监控,而区块链的防篡改特性也确保这个监控的正确性。

附图说明

[0063] 图1为本发明系统结构图;

[0064] 图2访问令牌授予过程

[0065] 图3访问令牌的分享过程

[0066] 图4访问令牌的委托过程

[0067] 图5带访问令牌的内容访问过程

[0068] 图6访问令牌的验证过程

具体实施方式

[0069] 下面结合附图和实施例对本发明作进一步说明。

[0070] 本发明包括访问交易格式、访问令牌的安全分发、访问令牌的撤销、内容访问的监控以及使用Cuckoo filter的快速检索。本发明基于区块链交易实现访问令牌安全分发和资源使用的有效监控,可以适用于任何使用访问令牌(或访问凭证)的访问控制系统,其结构如图1所示,具体实现过程如下:

[0071] 步骤1、设置访问交易格式

[0072] 在区块链中,每个交易都由三部分组成:交易标识(Tid)、交易的输入数组Tin[]和交易的输出数组Tout[]。而在本发明中,我们增加了一个新的字段:交易类型(Ttype),以便于快速查找某一交易记录而无需遍历整个区块链,而其中交易类型包括授予(Grant)、分享(Share)、委托(Delegate)、撤销(Revoke)和访问(Access),可表示为 $Ttype \in \{Grant, Share, Delegate, Revoke, Access\}$ 。因此,本发明中访问交易 T_{Ttype} 的交易格式用公式表示如公式(1)所示:

$$T_{Ttype} = (Tid, Ttype, Tin[PK_i, T_{pre}, \varphi], Tout[PK_j, AccToken, \omega]) \quad (1)$$

[0074] 在公式(1)中, PK_i, PK_j 分别表示交易的创建者和接收者地址; T_{pre} 表示访问令牌(AccToken)的上一次交易; φ 是一个输入脚本,用于获取之前交易的访问令牌; ω 是一个输出脚本,给出获取交易 T_{Ttype} 中所分发的访问令牌的条件。为了更加清晰的阐述,本发明的访问交易格式也可如表1所示。

[0075] 表1访问交易 T_{Ttype}

	$T_{Type} \text{ (in: } T_{pre} \text{)}$
交易类型:	$Ttype$
[0076] 访问令牌:	$AccToken$
输入脚本 ϕ:	$\phi \text{ or } Sig_{sk_{cp}}(T_{pre})$
输出脚本 $\varpi (body, \sigma)$:	$Ver_{PK_{CQ}}(body, \sigma)$

[0077] 在表1中, body包括 T_{pre} , $Ttype$, $AccToken$, PK_{CQ} ; σ 表示内容提供者对该访问交易的签名。如果该访问交易是一个初始交易, 那么它的输入交易为空, 可用 ϕ 表示。

[0078] 步骤2访问令牌的安全分发

[0079] 本发明根据不同的访问需求设计了3种访问令牌的分发方式, 并以区块链交易的形式进行访问令牌分发, 分别为: 访问令牌的授予 (Grant) 交易、访问令牌分享 (Share) 的交易和访问令牌的委托 (Delegate) 交易。

[0080] 2-1访问令牌的授予 (Grant) 交易

[0081] 当内容提供者第一次响应内容请求者的访问请求时, 内容提供者将访问令牌以授予访问令牌交易的方式分发给内容请求者, 访问令牌的授予的详细过程如图2所示, 具体过程如下:

[0082] (8) 内容请求者通过网络发送访问请求 (可以带一些身份标识数据, 具体根据所用的访问控制模型)。

[0083] (9) 内容提供者接收该请求, 身份认证通过之后为该请求者生成访问令牌。

[0084] (10) 内容提供者根据该访问令牌生成访问令牌的授予交易 T_{Grant} 如下所示:

$$[0085] \quad T_{Grant} = (Tid, Grant, Tin[PK_{cp}, \phi, \phi], Tout[PK_{CQ}, AccToken_g, \varpi]) \quad (2)$$

[0086] 在式子 (2) 中, T_{Grant} 是访问令牌 $AccToken$ 的初始交易, 因而它的 T_{pre} 和 ϕ 都为空, 可以记作 ϕ 。 T_{Grant} 用于访问令牌的授予, 所以它的访问类型为Grant。

[0087] (11) 该访问令牌的授予交易将被广播到区块链中。

[0088] (12) 矿工根据共识协议验证交易的有效性, 若有效则写入区块链中转入到步骤 (7), 否则拒绝进行步骤 (6)。

[0089] (13) 若交易被拒绝, 将会通知内容请求者, 内容请求者可再次发送请求。

[0090] (14) 内容请求者使用自身的私钥 SK_{CQ} 从区块链中获取访问令牌。

[0091] 而访问令牌的分享 (Share) 交易和委托 (Delegate) 交易中, 交易的广播和矿工验证方式以及访问令牌的获取方式和1-2相同, 将不再赘述。

[0092] 2-2访问令牌的分享 (Share) 交易

[0093] 当内容请求者B通过访问令牌授予交易从内容提供者A获取访问令牌之后, 如果内容请求者B拥有访问令牌的分享权限, B还可以将该访问令牌分享给其他请求者 (例如请求者C), 此时内容请求者B也被称为分享者B, 如图3所示。而分享者B可以通过访问令牌的分享交易 T_{Share} 将访问令牌分享给请求者C, 分享交易 T_{Share} 如下所示:

$$[0094] \quad T_{Share} = (Tid, Share, Tin[PK_B, T_{pre}, \phi], Tout[PK_C, AccToken, \varpi]) \quad (3)$$

[0095] 在式子(3)中, T_{pre} 是内容提供者A授予分享者B的访问令牌授予交易 T_{Grant} , PK_B , PK_C 分别表示分享者B和请求者C的地址。

[0096] 2-3访问令牌的委托(Delegate)交易

[0097] 访问令牌的委托交易用于处理当内容提供者A需要将该访问令牌通过该内容请求者D委托给第三方请求者C的情况,而此时内容请求者D也被称为委托者D,如图4所示。此过程首先内容提供者A通过令牌授予交易 T_{Grant} 将访问令牌分发给委托者D,然后委托者D生成访问令牌的委托交易 $T_{delegate}$,通过 $T_{delegate}$ 将访问令牌委托给第三方请求者C, $T_{delegate}$ 如下所示:

[0098]
$$T_{delegate} = (Tid, Delegate, Tin[PK_D, T_{pre}, \phi], Tout[PK_C, AccToken, \varpi]) \quad (4)$$

[0099] 在式子(4)中, T_{pre} 是内容提供者A授予委托者D的访问令牌授予交易 T_{Grant} , PK_D , PK_C 分别表示委托者D和第三方请求者C的地址。注意:委托者D有且只有一次可以把内容委托给第三方请求者C。

[0100] 步骤3访问令牌的撤销

[0101] 访问令牌的撤销可以分为两种情况:一是访问令牌的过期失效;二是在有效期内访问令牌的创建者主动撤销访问令牌。对于情况一:任何访问令牌的验证者都可以对已过期的访问令牌进行撤销;对于情况二:如果某一用户想要撤销由他自己授予、分享或委托的访问令牌,他可以生成访问令牌撤销交易 T_{revoke} ,如下所示:

[0102]
$$T_{revoke} = (Tid, Revoke, Tin[PK_{user}, T_{pre}, \phi], Tout[\phi, AccToken, \phi]) \quad (5)$$

[0103] 在式子(5)中, T_{pre} 表示该访问令牌上一次的交易, PK_{user} 表示启动该访问令牌撤销的用户的地址,输出地址和输出交易都设置为空(可以 ϕ 表示)是为了确保已撤销的访问令牌不再在区块链上传输。

[0104] 步骤4内容访问的监控

[0105] 内容请求者B使用已签名的访问令牌 $AccToken || \sigma$ 向内容提供者A发送请求以访问内容,内容提供者A先验证内容请求者B的访问令牌,之后为B提供内容同时A将生成内容访问交易 T_{access} ,如图5所示。访问令牌的验证过程(见图6)具体步骤如下所示:

[0106] 4-1. 令牌签名验证, A使用内容请求者B的公钥进行签名验证,若验证失败拒绝访问,否则继续验证。

[0107] 4-2. 时间验证, A验证访问令牌是否已过期,若是拒绝访问,否则继续验证。

[0108] 4-3. 撤销验证, A在区块链上检索该访问令牌的撤销交易,若存在说明该访问令牌已被撤销,拒绝访问,否则继续验证。

[0109] 4-4. 授予验证, A在区块链上检索该访问令牌的授予交易,若存在说明该访问令牌是合法令牌,可以为内容请求者B提供内容。

[0110] 如果内容请求者B通过以上的验证, A将为B提供访问内容之后将生成一个关于B使用该访问令牌的内容访问交易 T_{access} ,如下所示:

[0111]
$$T_{access} = (Tid, Access, Tin[PK_A, T_{pre}, \phi], Tout[PK_B, AccToken || access, \varpi]) \quad (6)$$

[0112] 在式子(6)中, T_{pre} 表示该访问令牌上一次的交易,输出数组 $Tout[]$ 中的 $AccToken || access$ 表示所使用的访问令牌和对应的内容访问操作。

[0113] 在本发明中,涉及访问令牌的所有操作都以交易的形式记录在区块链上。这些操

作包括访问令牌的分发(授予、分享和委托),使用访问令牌的内容访问操作以及访问令牌的撤销,这将组成一个全面的内容提供者的资源使用监控。内容提供者想要追责或者查询自己内容的访问情况都可以通过查找区块链获取,而区块链的防篡改特性也保证了资源使用监控的正确性。

[0114] 步骤5使用Cuckoo filter的快速交易检索

[0115] 为了提高区块链中交易记录的检索效率,本发明引入了Cuckoo filter。Cuckoo filter是一种高效的数据结构,支持动态添加和删除条目比Bloom filter拥有更好的检索性能和更少的空间使用率。一个Cuckoo filter由多个桶组成,而其中一个桶可以由多个实体,而每个实体存储一个指纹。对于添加条目 x ,先使用哈希函数计算两个候选桶 b_1 和 b_2 的索引如下所示(其中 $\text{fingerpr int}(x)$ 是 $\text{hash}(x)$ 的最低 k bits, M 表示桶的数量):

$$\begin{aligned} b_1 &= \text{hash}(x) \bmod M \\ [0116] \quad b_2 &= b_1 \oplus \text{hash}(\text{fingerprint}(x)) \bmod M \end{aligned} \quad (7)$$

[0117] 如果候选桶中有空桶,将 $\text{fingerpr int}(x)$ 保存到空桶中,否则,只需选择一个候选存储桶,删除它现有的条目,然后将此条目重新插入其候选桶中,重复该过程直到找到空桶或超过最大位移数。在Cuckoo filter中的查找过程是先给定条目 x ,然后根据式子(7)计算 $\text{fingerpr int}(x)$ 和两个候选桶,最后遍历两个候选桶,如果任一桶中的任何现有指纹匹配,返回true,否则返回false。在Cuckoo filter中删除条目过程为,先检查给定项 x 的两个候选桶,如果 $\text{fingerpr int}(x)$ 匹配任意一个候选桶中的条目,从该桶中删除该匹配 $\text{fingerpr int}(x)$ 的一个副本。

[0118] 在本发明中,我们分别为已授予的访问令牌和已撤销的访问令牌构建Cuckoo filter,分别记作 CF_g, CF_{inv} 。当矿工验证一个访问令牌授予交易成功后,他将该令牌的哈希 $H(\text{AccToken})$ 添加到 CF_g 同时将该交易写入区块链;而当矿工验证一个访问令牌撤销交易成功后,他只需从 CF_g 中删除 $H(\text{AccToken})$ 并将 $H(\text{AccToken})$ 添加到 CF_{inv} 同时将该交易写入区块链。这将提高用户在访问令牌验证过程的验证效率,用户无需再检索整个区块链以实现访问令牌的有效性验证,只需查询 CF_g, CF_{inv} 就可实现。

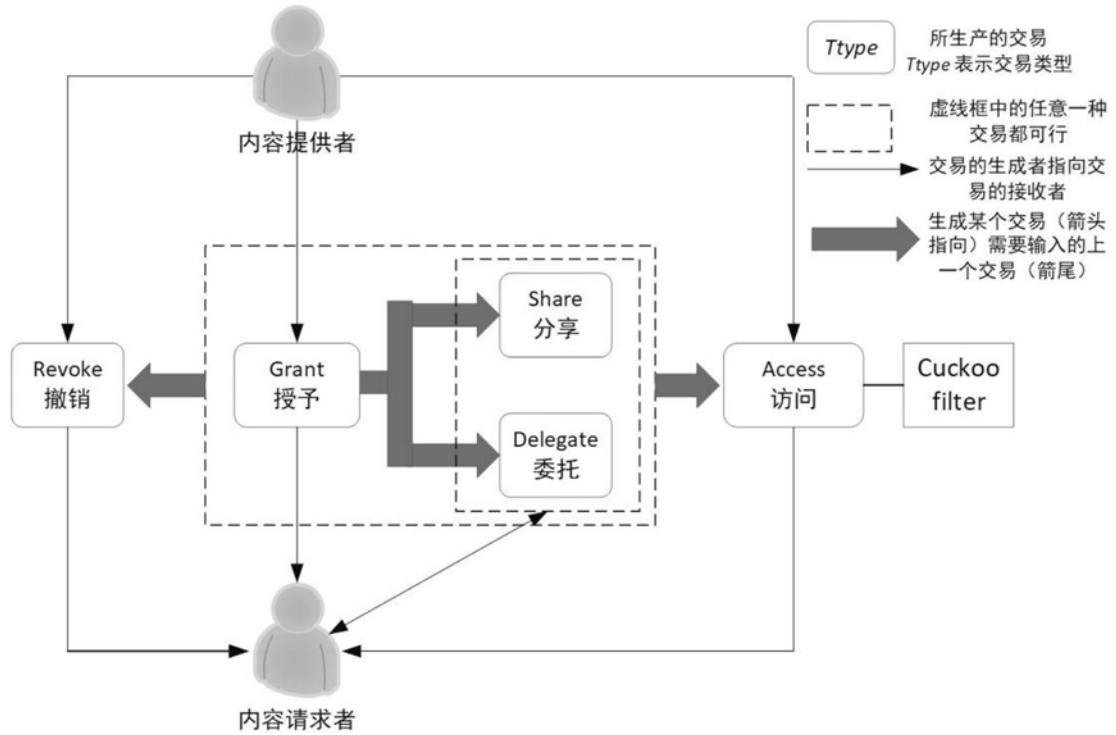


图1

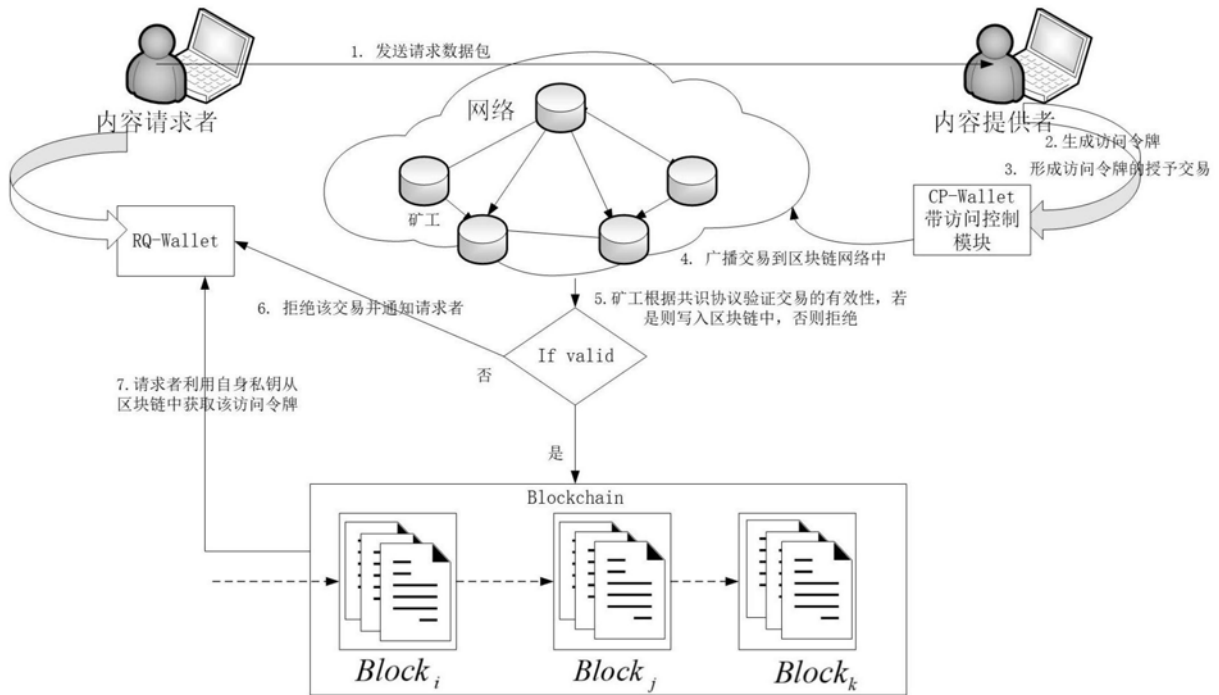


图2

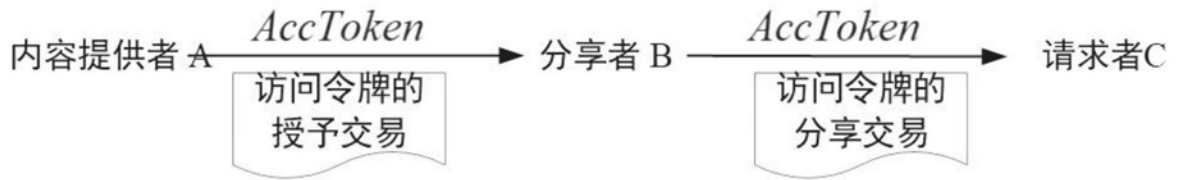


图3

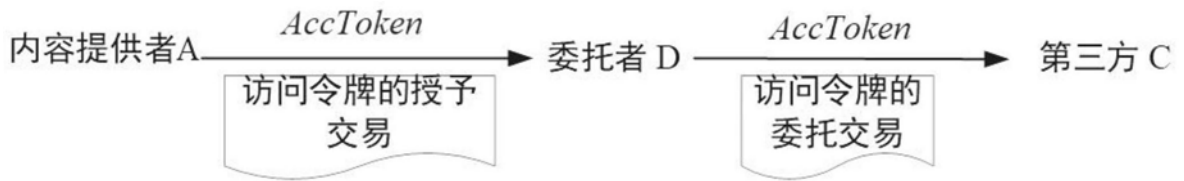


图4



图5

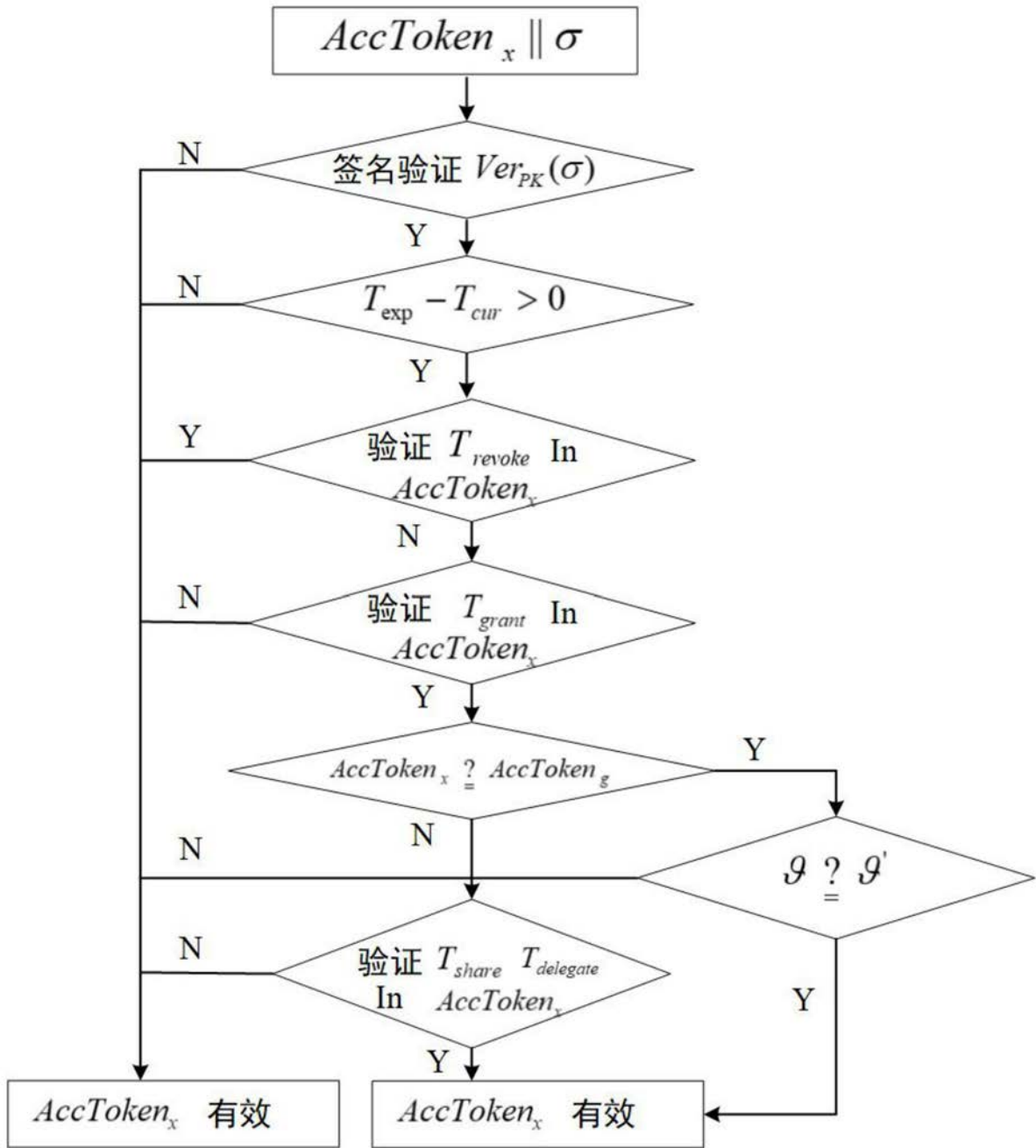


图6