(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109509095 A
(43)申请公布日 2019.03.22

(21)申请号 201811353900.9

(22)申请日 2018.11.14

(71)申请人 成都皓图智能科技有限责任公司
地址 610054 四川省成都市成华区一环路东一段159号电子信息产业大厦第603号房

(72)发明人 熊效李

(74)专利代理机构 成都虹盛汇泉专利代理有限公司 51268
代理人 王伟

(51)Int.Cl.
G06Q 40/04(2012.01)
G06Q 20/38(2012.01)
G06Q 20/06(2012.01)
G06K 9/00(2006.01)

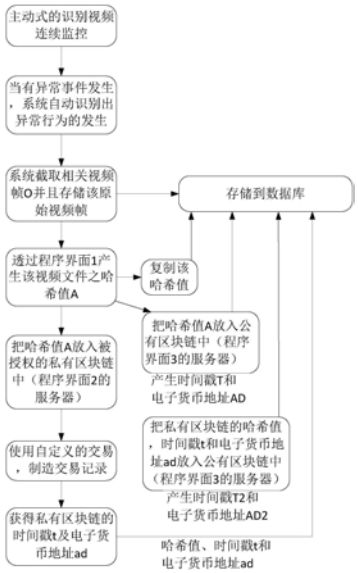
权利要求书1页 说明书5页 附图4页

(54)发明名称

一种结合区块链的视频主动识别方法

(57)摘要

本发明公开了一种结合区块链的视频主动识别方法，应用于视频识别领域，为了完整并真实性地保存视频文件，防止篡改；本发明结合公有区块链与私有区块链；公有区块链保证视频不可更改；私有区块链保证视频来源合法性；从而本发明的能够实现加密视频文件完整地、机密地、可认证地放在区块链上；并保持最原始地、具真实性以及可认证的视频特性，保存了该视频的真正价值，以及视频的不可更改特性。



CN 109509095 A

1.一种结合区块链的视频主动识别方法,其特征在于,包括:

S1、当有异常事件发生时,截取相关视频帧,作为原始视频文件;将该原始视频文件保存至数据库中;

S2、通过加密哈希函数为该原始视频文件产生哈希值;复制哈希值并存储到数据库中;

S3、将步骤S2产生的哈希值传送到私有区块链中;私有区块链使用自定义的交易,制造交易记录产生一私有电子货币地址,以及去中心可信任的第一交易时间戳;

S4、将步骤S2产生的哈希值传送到公有区块链中;公有区块链通过采用小额度的交易,制造交易记录产生第一非私有电子货币地址,以及去中心可信任的第二交易时间戳;将第一非私有电子货币地址、第二交易时间戳存放到数据库中;

S5、获取私有区块链的第一交易时间戳以及私有电子货币地址;分别存放到公有区块链与本地数据库中;

所述私有区块链的第一交易时间戳以及私有电子货币地址存放到公有区块链,公有区块链通过采用小额度的交易,制造交易记录产生第二非私有电子货币地址,以及去中心可信任的第三交易时间戳;并将第二非私有电子货币地址、第三交易时间戳存放到数据库中;

S6、将经步骤S2的加密哈希函数进行加密处理后的原始视频文件放入公有区块链;然后对视频文件进行验证。

2.根据权利要求1所述的一种结合区块链的视频主动识别方法,其特征在于,步骤S6所述对视频文件进行验证,包括对视频文件来源进行验证,具体为:

将存储在数据库中的哈希值与公有区块链中的哈希值对比;将存放在数据库中的私有区块链的第二交易时间戳、私有电子货币地址分别与公有区块链中存放的私有区块链的第二交易时间戳、私有电子货币地址进行对比;

若比对一致,则表示该视频文件来源合法,否则为非法。

3.根据权利要求1所述的一种结合区块链的视频主动识别方法,其特征在于,步骤S6所述对视频文件进行验证,还包括对视频文件是否被篡改进行验证,具体为:

将存放在公有区块链中的哈希值与存储在数据库中的哈希值对比;将存放在公有区块链中的第二交易时间戳与存储在数据库中的第二交易时间戳对比;将存放在公有区块链中的第三交易时间戳与存储在数据库中的第三交易时间戳对比;将存放在公有区块链中的第一非私有电子货币地址与存储在数据库中的第一非私有电子货币地址对比;将存放在公有区块链中的第二非私有电子货币地址与存放在数据库中的第二非私有电子货币地址对比;

若上述比对结果全部一致,则表示公有区块链中的原始视频文件未被篡改;否则被篡改。

一种结合区块链的视频主动识别方法

技术领域

[0001] 本发明涉及视频识别领域，具体涉及一种主动识别视频的技术。

背景技术

[0002] 对监控视频内容的完整性及真实性，不仅仅考验着技术层面的问题，也一直是安防监控贩售业者和使用者所关心的问题。随着时代的进步，视频记录也可以作为证据的一种形式来提供证明。但所围绕的关键问题依然是该视频的真实性及完整性。意指，该视频是否已经被更改过，它的可信度是被质疑的。只有保存视频帧的完整性及真实性才保存了视频帧本身的价值。

发明内容

[0003] 为解决上述技术问题，本发明提供了一种结合区块链的视频主动识别方法，结合公有区块链与具备限制访问权的私有区块链，实现不可更改的视频内容的效果。

[0004] 本发明采用的技术方案是：一种结合区块链的视频主动识别方法，包括：

[0005] S1、当有异常事件发生时，截取相关视频帧，作为原始视频文件；将该原始视频文件保存至数据库中；

[0006] S2、通过加密哈希函数为该原始视频文件产生哈希值；复制哈希值并存储到数据库中；

[0007] S3、将步骤S2产生的哈希值传送到私有区块链中；私有区块链使用自定义的交易，制造交易记录产生一私有电子货币地址，以及去中心可信任的第一交易时间戳；

[0008] S4、将步骤S2产生的哈希值传送到公有区块链中；公有区块链通过采用小额度的交易，制造交易记录产生第一非私有电子货币地址，以及去中心可信任的第二交易时间戳；将第一非私有电子货币地址、第二交易时间戳存放到数据库中；

[0009] S5、获取私有区块链的第一交易时间戳以及私有电子货币地址；分别存放到公有区块链与本地数据库中；

[0010] 所述私有区块链的第一交易时间戳以及私有电子货币地址存放到公有区块链，公有区块链通过采用小额度的交易，制造交易记录产生第二非私有电子货币地址，以及去中心可信任的第三交易时间戳；并将第二非私有电子货币地址、第三交易时间戳存放到数据库中；

[0011] S6、将经步骤S2的加密哈希函数进行加密处理后的原始视频文件放入公有区块链；然后对视频文件进行验证。

[0012] 进一步地，步骤S6所述对视频文件进行验证，包括对视频文件来源进行验证，具体为：

[0013] 将存储在数据库中的哈希值与公有区块链中的哈希值对比；将存放在数据库中的私有区块链的第二交易时间戳、私有电子货币地址与公有区块链中存放的私有区块链的第二交易时间戳、私有电子货币地址进行对比；

[0014] 若比对一致，则表示该视频文件来源合法，否则为非法。

[0015] 进一步地，步骤S6所述对视频文件进行验证，还包括对视频文件是否被篡改进行验证，具体为：

[0016] 将存放在公有区块链中的哈希值与存储在数据库中的哈希值对比；将存放在公有区块链中的第二交易时间戳与存储在数据库中的第二交易时间戳对比；将存放在公有区块链中的第三交易时间戳与存储在数据库中的第三交易时间戳对比；将存放在公有区块链中的第一非私有电子货币地址与存储在数据库中的第一非私有电子货币地址对比；将存放在公有区块链中的第二非私有电子货币地址与存放在数据库中的第二非私有电子货币地址对比；

[0017] 若上述比对结果全部一致，则表示公有区块链中的原始视频文件未被篡改；否则被篡改。

[0018] 本发明的有益效果：本发明的一种结合区块链的视频主动识别方法，考虑到公有区块链的服务可能造成的延迟影响；虽然公有区块链上保证了最大地视频的不可更改性，但该服务的延迟影响，可能无法证明该视频内容发生的第一时间，因此本发明使用了一道私有区块链服务；从而，经过主动式的视频识别检测到的异常事件记录视频，可以完整地、机密地、可认证地放在区块链上，保持最原始地、具真实性以及可认证的视频特性，保存了该视频的真正价值，以及视频的不可更改特性。

附图说明

[0019] 图1为本发明实施例提供的方案流程图；

[0020] 图2为本发明实施例提供的采用密哈希函数(MD5)产生哈希值的示意图；

[0021] 图3为本发明实施例提供的区块链的结构示意图；

[0022] 图4为本发明实施例提供的为添加时间戳的原始视频文件产生哈希值的流程图。

具体实施方式

[0023] 以下结合附图对本发明的内容做进一步阐述。

[0024] 如图1所示为本发明的方案流程图，本发明的技术方案为：一种结合区块链的视频主动识别方法，包括：

[0025] S1、当有异常事件发生时，截取相关视频帧0，作为原始视频文件；将该原始视频文件保存至数据库中；使用软件应用程序来执行监控、计算并且分析目标对象来进行识别。当异常行为发生时(例如，打架、拿刀杀人、撞车、摔倒、撞墙等)会触发前端系统识别出来，当系统检测有异常事件时，摄像头系统会截取相关视频帧数据；并对提取出来的原始视频数据进行保存；

[0026] S2、通过加密哈希函数为该原始视频文件产生哈希值A；复制哈希值A并存储到数据库中；

[0027] 使用哈希加密算法(例如MD5等)产生所相对应的哈希值A；如图2所示，加密的哈希函数可将任意长度的二进制值映射为较短的固定长度的二进制值，例如MD5(在此处我们使用MD5为例子)可产生128比特，而经过MD5的转换结果为32十六进制字符。即任一长度的二进制输入，经过MD5的转换后都产生为32十六进制字符。在输入的二进制文件中，即使有小

小的一个字符变动，也可以造成输出十六进制字符的大大改变。此结果是明显，明确可观察到的。再者，两个不同的字符串要产生完全相同的哈希值接近于不可能实现。

[0028] 加密哈希函数具备以下特性：1)无法去更改了一原始数据而不会更改其所产生的哈希值。2)无法去从一原始数据所产生的哈希值来还原该原始数据。3)可以轻易地从任一原始数据产生其哈希值。4)无法从两个不一致、不相同的原始数据来产生相同的哈希值。在加密哈希函数中有着许多安全上的应用，例如信息认证码、数字签名等。这些应用像是作为校验和来确认文件的一致性。而哈希值有时候也可称作数字指纹。

[0029] 为原始视频文件产生哈希值，具体过程为：例如若视频每秒可以产生出一哈希值，而视频图像是每秒30帧记录的方式。现有一侦测到的异常事件视频内容有三分钟长，则将会产生总数为5400帧的视频。如果前置设定时间间隔为一秒，那将会产生180个数据区块，就相当于产生了尽不相同的180个哈希值。这些连续产生的180个哈希值可以在哈希值结构树中用一主要的哈希值(Master Hash)来代表该三分钟视频的内容数据。

[0030] 以下具体阐述结合公有区块链与私有区块链，保存了该视频的真正价值，以及视频的不可更改特性。

[0031] 首先，不论公有区块链还是私有区块链均为一对等网络，其去中心化的开放式账本；譬如比特币结构，依赖于一分布式共享网络存在于各用户之间。每一用户拥有自己的公开账本都记录着每一笔交易，而基于应用在该网络结构上，可以作到确信其当检验与其他使用者交易记录时的正确性。该一账本就称作区块链。

[0032] 在传统的交易方式中，需要一第三方机构，其使用的是中心化网络中的一中心节点执行审计和作为负责交易的角色。区块键是一公开账本并记录着比特币或加密电子货币的交易，来取代传统的交易方式。要实施这样不需要任何可信任的中心机构，完成每一交易记录的真实性，是透过对等网络上的每一节点在区块链的结构上执行比特币或相关软件来达成。举例一种交易的形式，当甲方给乙方3个比特币，再使用一简单可得的软件应用程序把该交易记录广播到该网络。网络上的多数节点能够验证该交易记录并且添加该交易记录的副本到每个自己的公开账本上，再把这些账本广播到其他该网络的节点上。该区块链就相当于一分布上的数据库。为了达到能独立地验证其区块链上的每一节点上的所有权或验证任何一节点上比特币的数量，任一网络上的节点自己都有存储在该区块链上的副本。当一新的交易记录接收时，一个区块就被创造并添加在该区块链里，然后迅速地公开在所有节点上。在传统的交易方式中，因为有了中心化的第三方机构，所以第三方保留了交易总账从而确保每一交易是否已花掉或提取.

[0033] 如图3所示，在区块链当中，每一区块都包含了上一个区块的哈希值，从创造区块开始连接到当前区块从而形成块链。每一个区块都确保按时间顺序在上个区块之后产生，否则前一个区块的哈希值是未知的。同时所有交易在该区块链中都要对外进行广播，所以只有当包含在最新区块中的所有交易都是独一无二且之前从未发生过，其他节点才会认可该区块。因此在区块链中，用该方法确保每一交易是否花掉或提取。

[0034] S3、将步骤S2产生的哈希值A传送到私有区块链中；私有区块链使用自定义的交易，制造交易记录产生一私有电子货币地址ad，以及去中心可信任的第一交易时间戳t；具体的过程如图1所示，包括：将步骤S2产生的哈希值A传送到程序界面2的服务器，该服务器为提供私有电子货币的私有区块链服务。在该服务器使用自定义的交易来从该交易记录产

生一私有电子货币地址ad，也产生了一去中心可信任的第一交易时间戳t，则该视频的内容，即哈希值A和交易时间的时间戳t就持久地并且不可更改地存储在私有区块键里。

[0035] 哈希值A存储在私有区块键里，让该视频帧内容有着不可更改的特性以及信息隐秘性；对应存储在私有区块键里的第一交易时间戳t及私有电子货币地址ad，让该视频内容有着不可更改的特性。

[0036] 相比较于公有区块链，任何人都可以参与记账过程，私有区块链可以限制谁拥有访问权。因为公有区块链任何人都可以参与账本记录的过程，也就是说任何人根据区块链上面所述的特性，都可以在上面存储视频帧，也可达到不可更改的目的。但是并无法对公有区块链上所存储视频帧的来源所属(或是传送至公有区块链的中间过程被替换视频帧)或是已经造假的视频帧上传到区块链里面的认证性质作到完善。为了认证该已经上传到区块链的视频帧的来源为真实地，在此利用了私有区块链的可认证性质，当作一种形式的认证签名发送到公有区块链里面。

[0037] S4、将步骤S2产生的哈希值传送到公有区块链中；公有区块链通过采用小额度的交易，制造交易记录产生第一非私有电子货币地址，以及去中心可信任的第二交易时间戳；将第一非私有电子货币地址、第二交易时间戳存放到数据库中；具体的过程如图1所示，包括：

[0038] 在将哈希值A传送到程序界面2的服务器同时，把哈希值A也传送到程序界面3的服务器。该服务器为提供非私有电子货币的公有区块链服务。该服务器使用小额度的交易来从该交易记录产生一非私有电子货币地址AD，也产生了一去中心可信任的第二交易时间戳T，则该视频的内容，即哈希值A和第二交易时间戳T就持久地并且不可更改地存储在公有区块键里。

[0039] 哈希值A存储在公有区块键里，让该视频帧内容有着不可更改的特性以及信息隐秘性；因此所对应存储在公有区块键里的第二交易时间戳T及非私有电子货币地址AD，让该视频内容有着不可更改的特性。

[0040] S5、获取私有区块链的第一交易时间戳以及私有电子货币地址；分别存放到公有区块链与本地数据库中；

[0041] 所述私有区块链的第一交易时间戳t以及私有电子货币地址ad存放到公有区块链，公有区块链通过采用小额度的交易，制造交易记录产生第二非私有电子货币地址AD2，以及去中心可信任的第三交易时间戳T2；并将第二非私有电子货币地址AD2、第三交易时间戳T2存放到数据库中。

[0042] 如图4所示，原始相关视频帧0透过程序界面1产生该视频文件的哈希值A，放入公有区块链中，可以在公有区块链里附近几个时间区块找到从私有区块链获得的第一交易时间戳t及电子货币地址ad的区块(之后放入公有区块链中)。该方法作为认证签名的一种手段来证明发布在公有区块链的视频帧来源是已经得到私有区块链许可的成员。

[0043] 反之，原始相关视频帧X透过程序界面1产生该视频文件的哈希值B，放入公有区块链中，不能够在公有区块链里附近几个时间区块找到所对应的私有区块链认证信息。可以说明放入该视频帧的来源并不属于真正的拥有者。

[0044] S6、将经步骤S2的加密哈希函数进行加密处理后的原始视频文件放入公有区块链；然后对视频文件进行验证。

[0045] 为了去证明视频的内容没有被窜改或更改,使用哈希值的对比。

[0046] 使用存储本地数据库的哈希值A和放入公有区块链的哈希值对比。

[0047] 使用存储本地数据库的私有区块链的第一交易时间戳t及电子货币地址ad和之前放入公有区块链的值对比。

[0048] 如果放在公有区块链的t及ad是和本地数据库存储的一致的话,代表来源是正确的。

[0049] 也可用放在区块链上的哈希值以及交易后所产生出来的去中心可信任时间戳T、T2,电子货币地址AD,AD2来和已经存储在数据库的哈希值,去中心可信任的时间戳T、T2,电子货币地址AD,AD2作对比;若一致则表示未被篡改,否则被篡改。

[0050] 对比的方法可以透过包括像是透过服务器,或使用相关区块键检测工具或其他软件程序等方考虑了公有区块链的服务可能造成的延迟影响。虽然公有区块链上保证了最大地视频的不可更改性,但该服务的延迟影响,可能无法证明该视频内容发生的第一时间,所以使用了一道的私有区块链的服务。

[0051] 因而,经过主动式的视频识别检测到的异常事件记录视频,可以完整地、机密地、可认证地放在区块链上,保持最原始地、具真实性以及可认证的视频特性,保存了该视频的真正价值,以及视频的不可更改特性。

[0052] 本领域的普通技术人员将会意识到,这里所述的实施例是为了帮助读者理解本发明的原理,应被理解为本发明的保护范围并不局限于这样的特别陈述和实施例。对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的权利要求范围之内。

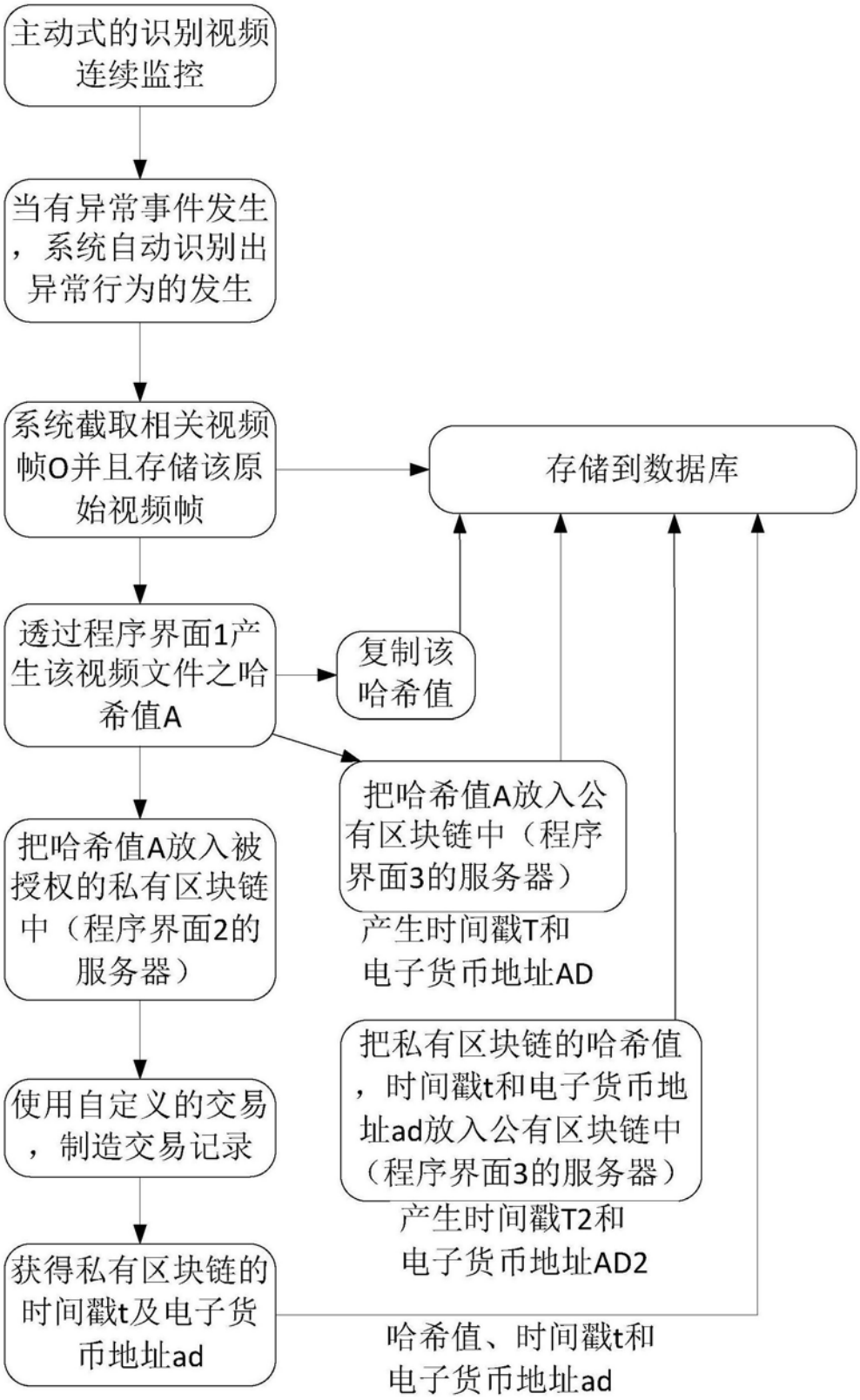

主动式的识别视频连续监控
当有异常事件发生，系统自动识别出异常行为的发生
系统截取相关视频帧O并且存储该原始视频帧
存储到数据库
透过程序界面1产生该视频文件之哈希值A
复制该哈希值
把哈希值A放入公有区块链中（程序界面3的服务器）
产生时间戳T和电子货币地址AD
把哈希值A放入被授权的私有区块链中（程序界面2的服务器）
把私有区块链的哈希值，时间戳t和电子货币地址ad放入公有区块链中（程序界面3的服务器）
产生时间戳T2和电子货币地址AD2
使用自定义的交易，制造交易记录
获得私有区块链的时间戳t及电子货币地址ad
哈希值、时间戳t和电子货币地址ad

图1


原始数据
哈希值
3947820920555
加密哈希函数
7bc97615d9f6981949c3efd2f28b1237
3947820920555
加密哈希函数
0ba8a83dca96e9ca150becc7d4b68d45
3947820920555
加密哈希函数
3b8cd58ca7664f2d306e2327fd125e33

图2

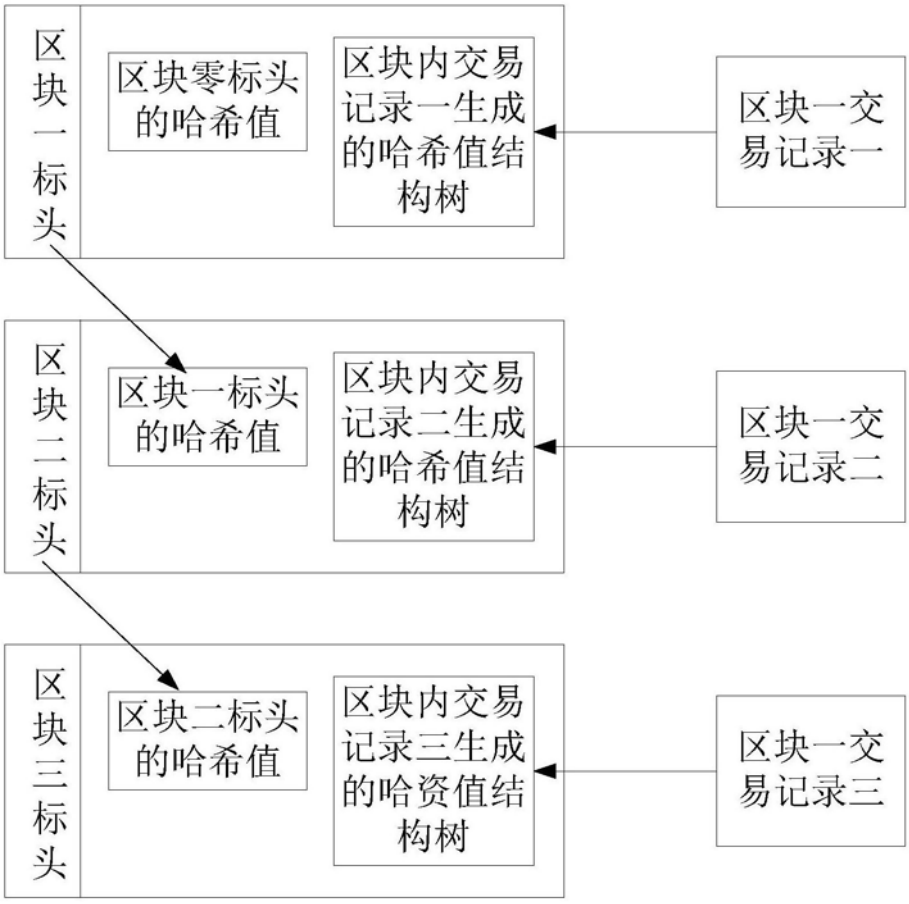

区块一标头
区块零标头的哈希值
区块内交易记录一生成的哈希值结构树
区块一交易记录一
区块二标头
区块一标头的哈希值
区块内交易记录二生成的哈希值结构树
区块一交易记录二
区块三标头
区块二标头的哈希值
区块内交易记录三生成的哈资值结构树
区块一交易记录三

图3

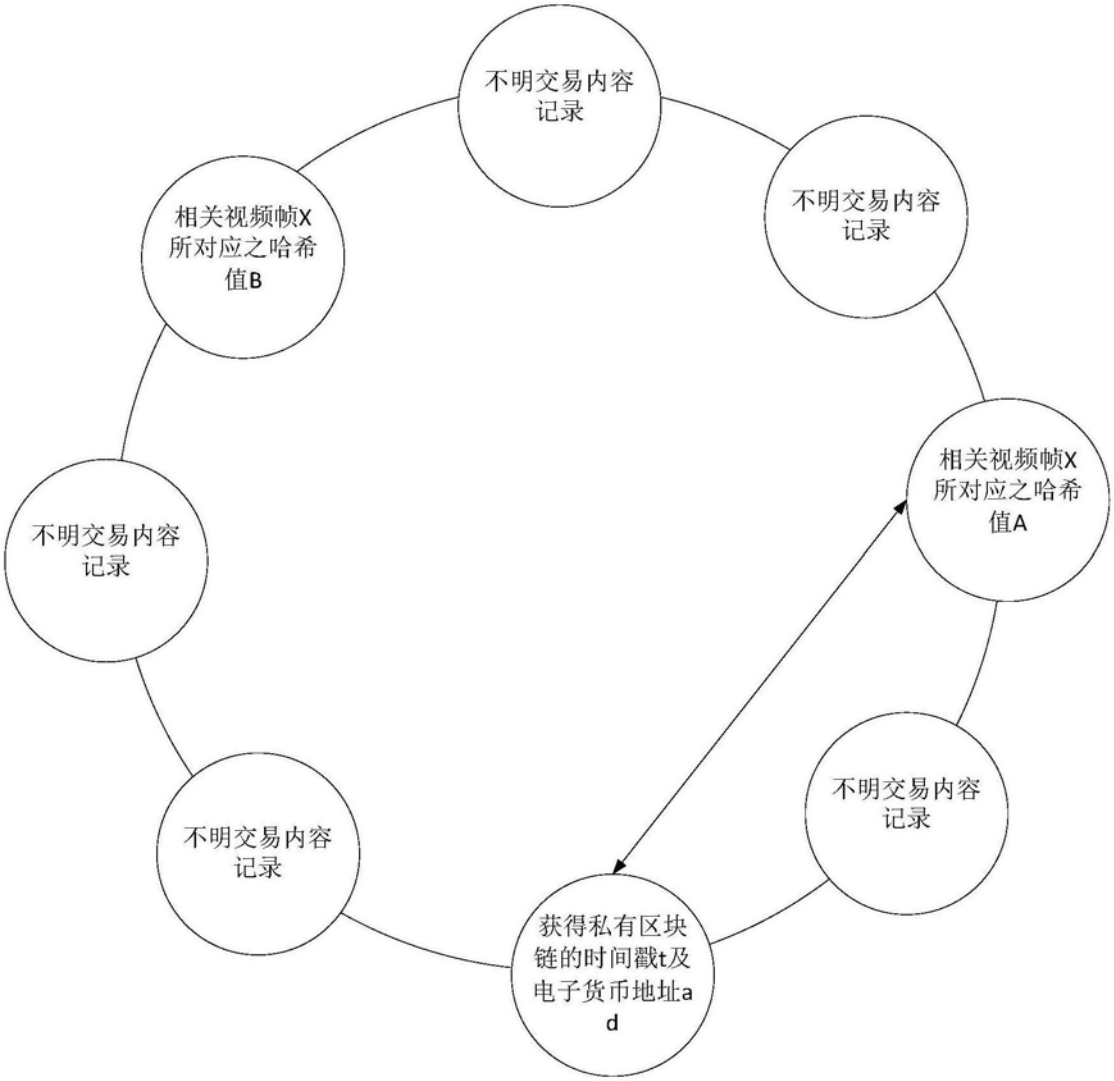

不明交易内容记录
不明交易内容记录
相关视频帧X所对应之哈希值A
不明交易内容记录
获得私有区块链的时间戳t及电子货币地址ad
不明交易内容记录
不明交易内容记录
相关视频帧X所对应之哈希值B

图4