(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116366232 B
(45)授权公告日 2024.10.11

(21)申请号 202310296844.4
(22)申请日 2023.03.24
(65)同一申请的已公布的文献号
申请公布号 CN 116366232 A
(43)申请公布日 2023.06.30
(73)专利权人 国开启科量子技术(北京)有限公司
地址 100193 北京市海淀区西北旺东路10号院东区5号楼一层108
专利权人 启科量子技术(珠海)有限公司
(72)发明人 曾祥洪 周卓俊 韩琢 罗乐
(74)专利代理机构 北京威禾知识产权代理有限公司 11838
专利代理师 王月玲
(51)Int.Cl.
H04L 9/06(2006.01)
G06F 21/64(2013.01)
G06F 21/60(2013.01)
H04L 9/08(2006.01)
H04L 9/30(2006.01)
H04L 9/32(2006.01)
(56)对比文件
CN 103916238 A,2014.07.09
CN 110011790 A,2019.07.12
审查员 王婕

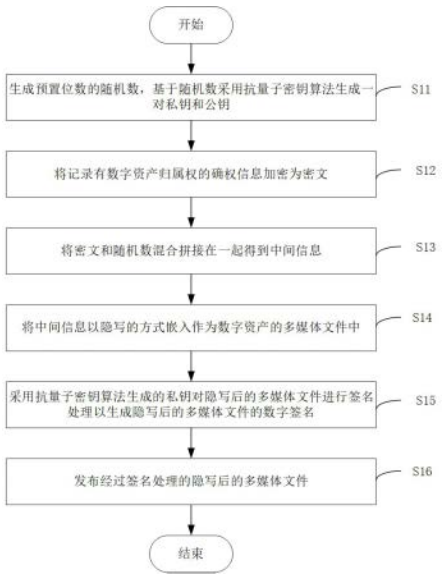
权利要求书3页 说明书14页 附图5页

(54)发明名称

基于抗量子密钥的数字资产处理方法、装置、设备及介质

(57)摘要

本发明公开了基于抗量子密钥的数字资产处理方法、装置、设备及介质,所述处理方法包括:生成预置位数的随机数,并基于随机数采用抗量子密钥算法生成一对私钥和公钥;将记录有数字资产归属权的确权信息加密为密文;将密文和随机数混合拼接在一起得到中间信息;将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中;采用抗量子密钥算法生成的私钥对隐写后的多媒体文件进行签名处理以生成隐写后的多媒体文件的数字签名;以及发布经过签名处理的隐写后的多媒体文件。本发明处理的多媒体文件种中所隐含的确权信息不仅具有高的不可破解性,而且能够为数字资产的合法持有者进行有效确权。



CN 116366232 B

1.一种基于抗量子密钥的数字资产处理方法,其特征在于,包括:

生成预置位数的随机数,并基于随机数采用抗量子密钥算法生成一对第一私钥和第一公钥;

将记录有数字资产归属权的确权信息加密为密文;

将密文和随机数混合拼接在一起得到中间信息;

将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中;

采用抗量子密钥算法生成的第一私钥对隐写后的多媒体文件进行签名处理以生成隐写后的多媒体文件的数字签名;以及

发布经过签名处理的隐写后的多媒体文件;

其中,采用抗量子密钥算法生成的与第一私钥相应的第一公钥被配置为在对发布的多媒体文件确权时对发布的多媒体文件的数字签名进行验证。

2.根据权利要求1所述的基于抗量子密钥的数字资产处理方法,其特征在于,确权信息的表现形式包括文本、图片、音频、视频和数字摘要中的至少一者。

3.根据权利要求1所述的基于抗量子密钥的数字资产处理方法,其特征在于,发布经过签名处理的隐写后的多媒体文件的步骤包括:

将隐写后的多媒体文件数据拼接在作为数字资产的多媒体文件数据后;

扰乱拼接处的数据块,数据块包括作为数字资产的多媒体文件尾部的部分数据块和隐写后的多媒体文件头部的部分数据块;以及

发布拼接在作为数字资产的多媒体文件数据后且拼接处的数据块被扰乱的隐写后的多媒体文件。

4.根据权利要求1所述的基于抗量子密钥的数字资产处理方法,其特征在于,将记录有数字资产归属权的确权信息加密为密文的步骤包括:

生成预置位数的另一随机数,基于另一随机数采用抗量子密钥算法生成一对第二私钥和第二公钥;以及

采用抗量子密钥算法生成的第二公钥对记录有数字资产归属权的确权信息进行加密;

其中,采用抗量子密钥算法生成的与第二公钥相应的第二私钥被配置为在对发布的多媒体文件确权时解密混合拼接在以隐写的方式嵌入发布的多媒体文件中的中间信息中的密文。

5.根据权利要求1所述的基于抗量子密钥的数字资产处理方法,其特征在于,抗量子密钥算法包括基于格的算法、基于编码的算法、基于多变量的算法和基于哈希的算法中的至少一种。

6.一种基于抗量子密钥的数字资产处理方法,其特征在于,包括:

采用抗量子密钥算法生成的第一公钥对待确权的多媒体文件的数字签名进行验证;

响应于待确权的多媒体文件的数字签名通过验证,对待确权的多媒体文件进行反隐写处理;

响应于对待确权的多媒体文件进行反隐写处理得到中间信息,对中间信息进行拆分处理;

响应于对中间信息进行拆分处理得到密文,对密文进行解密;

响应于对密文进行解密得到确权信息,将解密得到的确权信息与待确权的多媒体文件

所对应的数字资产归属权进行对比;以及

响应于解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权一致,确定待确权的多媒体文件通过归属权确权;

其中,采用抗量子密钥算法生成的与第一公钥相应的第一私钥被配置为在发布待确权的多媒体文件时生成待确权的多媒体文件的数字签名。

7.根据权利要求6所述的基于抗量子密钥的数字资产处理方法,其特征在于,还包括:

响应于待确权的多媒体文件的数字签名没有通过验证,确定待确权的多媒体文件没有通过归属权确权;或者

响应于对待确权的多媒体文件进行反隐写处理没有得到中间信息,确定待确权的多媒体文件没有通过归属权确权;或者

响应于对中间信息进行拆分处理没有得到密文,确定待确权的多媒体文件没有通过归属权确权;或者

响应于对密文进行解密没有得到确权信息,确定待确权的多媒体文件没有通过归属权确权;或者

响应于解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权不一致,确定待确权的多媒体文件没有通过归属权确权。

8.根据权利要求6所述的基于抗量子密钥的数字资产处理方法,其特征在于,对密文进行解密的步骤包括:

采用抗量子密钥算法生成的第二私钥对密文进行解密,其中,采用抗量子密钥算法生成的与第二私钥相应的第二公钥被配置为在发布待确权的多媒体文件时将确权信息加密成混合拼接在以隐写的方式嵌入待确权的多媒体文件中的中间信息中的密文。

9.根据权利要求6所述的基于抗量子密钥的数字资产处理方法,其特征在于,对待确权的多媒体文件进行反隐写处理的步骤包括:

恢复待确权的多媒体文件中的拼接处的数据;以及

基于拼接处的数据中的头部数据向后提取出隐写后的多媒体文件;

对提取出的隐写后的多媒体文件进行反隐写处理。

10.一种基于抗量子密钥的数字资产处理装置,其特征在于,包括:

密钥单元,被配置为生成预置位数的随机数,并基于随机数采用抗量子密钥算法生成一对私钥和公钥;

加密单元,被配置为将记录有数字资产归属权的确权信息加密为密文;

拼接单元,被配置为将密文和随机数混合拼接在一起得到中间信息;

隐写单元,被配置为将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中;

签名单元,被配置为采用抗量子密钥算法生成的私钥对隐写后的多媒体文件进行签名处理以生成隐写后的多媒体文件的数字签名;以及

发布单元,被配置为发布经过签名处理的隐写后的多媒体文件;

其中,采用抗量子密钥算法生成的与私钥相应的公钥被配置为在对发布的多媒体文件确权时对发布的多媒体文件的数字签名进行验证。

11.一种基于抗量子密钥的数字资产处理装置, 其特征在于,包括:

签名验证单元,被配置为采用抗量子密钥算法生成的公钥对待确权的多媒体文件的数

字签名进行验证;

反隐写单元,被配置为响应于待确权的多媒体文件的数字签名通过验证,对待确权的多媒体文件进行反隐写处理;

拆分单元,被配置为响应于对待确权的多媒体文件进行反隐写处理得到中间信息,对中间信息进行拆分处理;

解密单元,被配置为响应于对中间信息进行拆分处理得到密文,对密文进行解密;

对比单元,被配置为响应于对密文进行解密得到确权信息,将解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权进行对比;以及

确权单元,被配置为响应于解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权一致,确定待确权的多媒体文件通过归属权确权;

其中,采用抗量子密钥算法生成的与公钥相应的私钥被配置为在发布待确权的多媒体文件时生成待确权的多媒体文件的数字签名。

12.根据权利要求11所述的基于抗量子密钥的数字资产处理装置, 其特征在于,确权单元还被配置为:

响应于待确权的多媒体文件的数字签名没有通过验证,确定待确权的多媒体文件没有通过归属权确权;或者

响应于对待确权的多媒体文件进行反隐写处理没有得到中间信息,确定待确权的多媒体文件没有通过归属权确权;或者

响应于对中间信息进行拆分处理没有得到密文,确定待确权的多媒体文件没有通过归属权确权;或者

响应于对密文进行解密没有得到确权信息,确定待确权的多媒体文件没有通过归属权确权;或者

响应于解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权不一致,确定待确权的多媒体文件没有通过归属权确权。

13.一种电子设备,其特征在于,包括处理器以及存储有计算机程序指令的存储器;处理器执行计算机程序指令时实现如权利要求1-9中任一项所述的基于抗量子密钥的数字资产处理方法。

14.一种计算机可读存储介质,其特征在于,计算机存储介质上存储有计算机程序指令,计算机程序指令被处理器执行时实现如权利要求1-9中任一项所述的基于抗量子密钥的数字资产处理方法。

基于抗量子密钥的数字资产处理方法、装置、设备及介质

技术领域

[0001] 本发明涉及抗量子计算技术领域,尤其涉及基于抗量子密钥的数字资产处理方法、装置、设备及介质。

背景技术

[0002] 数字资产是一种以数字形式展现和流转的、包含全量信息的资产,如非同质化通证(Non-Fungible Token,简称NFT)和数字藏品。其中,NFT是一种基于公链、符合相关规范的非可互换通证,可以与某件虚拟数字物品关联成唯一的指代关系,因而单个发行的 NFT 不可以相互交换,具有全球唯一性,并可以通过虚拟货币交易。与NFT类似,数字藏品通常是指基于联盟链的指定作品、艺术品、商品的唯一数字标识,不能通过虚拟货币交易。NFT和数字藏品在区块链上的表现形式包括但不限于数字画作、图片、音乐、视频、3D模型(简称为多媒体文件)等,为方便说明,将这些表现形式统称为多媒体文件。

[0003] 作为在网络上公开流转的多媒体文件,其数字内容极其容易被非法复制和分发,因而常容易出现在一个平台发行的数字资产的数字内容被用于另一个平台的情况,而数字内容的创作者要证明其是数字内容的创作者的难度大,成本高。

发明内容

[0004] 有鉴于此,本发明实施例提供了基于抗量子密钥的数字资产处理方法、装置、设备及介质,至少用于解决数字资产归属权确权难度大的问题。

[0005] 根据本发明的一个方面,本发明提供了一种基于抗量子密钥的数字资产处理方法,包括以下步骤:生成预置位数的随机数,并基于随机数采用抗量子密钥算法生成一对第一私钥和第一公钥;将记录有数字资产归属权的确权信息加密为密文;将密文和随机数混合拼接在一起得到中间信息;将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中;采用抗量子密钥算法生成的第一私钥对隐写后的多媒体文件进行签名处理以生成隐写后的多媒体文件的数字签名;以及发布经过签名处理的隐写后的多媒体文件;其中,采用抗量子密钥算法生成的与第一私钥相应的第一公钥被配置为在对发布的多媒体文件确权时对发布的多媒体文件的数字签名进行验证。

[0006] 根据本发明的另一方面,本发明还提供了一种基于抗量子密钥的数字资产处理方法,包括以下步骤:采用抗量子密钥算法生成的第一公钥对待确权的多媒体文件的数字签名进行验证;响应于待确权的多媒体文件的数字签名通过验证,对待确权的多媒体文件进行反隐写处理;响应于对待确权的多媒体文件进行反隐写处理得到中间信息,对中间信息进行拆分处理;响应于对中间信息进行拆分处理得到密文,对密文进行解密;响应于对密文进行解密得到确权信息,将解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权进行对比;以及响应于解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权一致,确定待确权的多媒体文件通过归属权确权;其中,采用抗量子密钥算法生成的与第一公钥相应的第一私钥被配置为在发布待确权的多媒体文件时生成待确权的多媒

体文件的数字签名。

[0007] 根据本发明的另一方面,本发明还提供了一种基于抗量子密钥的数字资产处理装置,包括密钥单元、加密单元、拼接单元、隐写单元、签名单元和发布单元,其中,密钥单元被配置为生成预置位数的随机数,并基于随机数采用抗量子密钥算法生成一对私钥和公钥;加密单元被配置为将记录有数字资产归属权的确权信息加密为密文;拼接单元被配置为将密文和随机数混合拼接在一起得到中间信息;隐写单元被配置为将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中;签名单元被配置为采用抗量子密钥算法生成的私钥对隐写后的多媒体文件进行签名处理以生成隐写后的多媒体文件的数字签名;发布单元被配置为发布经过签名处理的隐写后的多媒体文件;其中,采用抗量子密钥算法生成的与私钥相应的公钥被配置为在对发布的多媒体文件确权时对发布的多媒体文件的数字签名进行验证。

[0008] 根据本发明的另一方面,本发明还提供了一种基于抗量子密钥的数字资产处理装置,包括签名验证单元、反隐写单元、拆分单元、解密单元、对比单元和确权单元,其中,签名验证单元被配置为采用抗量子密钥算法生成的公钥对待确权的多媒体文件的数字签名进行验证;反隐写单元被配置为响应于待确权的多媒体文件的数字签名通过验证,对待确权的多媒体文件进行反隐写处理;拆分单元被配置为响应于对待确权的多媒体文件进行反隐写处理得到中间信息,对中间信息进行拆分处理;解密单元被配置为响应于对中间信息进行拆分处理得到密文,对密文进行解密;对比单元被配置为响应于对密文进行解密得到确权信息,将解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权进行对比;确权单元被配置为响应于解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权一致,确定待确权的多媒体文件通过归属权确权;其中,采用抗量子密钥算法生成的与公钥相应的私钥被配置为在发布待确权的多媒体文件时生成待确权的多媒体文件的数字签名。

[0009] 根据本发明的另一方面,本发明还提供了一种电子设备,包括处理器以及存储有计算机程序指令的存储器;处理器执行计算机程序指令时实现了前述的基于抗量子密钥的数字资产处理方法。

[0010] 根据本发明的另一方面,本发明还提供了一种计算机可读存储介质,计算机存储介质上存储有计算机程序指令,计算机程序指令被处理器执行时实现了前述的基于抗量子密钥的数字资产处理方法。

[0011] 本发明提供的方法、装置、设备及介质能够在数字资产上链前对其进行处理,这既不影响数字资产的正常公布与交易,也能在需要确权时进行快速确权,处理速度快、准确。由于本发明对数字资产进行的处理既包括采用抗量子密钥进行签名的步骤,又包括多个进一步处理步骤,如拼接、隐写等,因而使得经过本发明处理后的数字资产具有不可破解性,也就防止了他人伪造相同处理方式来模仿数字资产的可能性。在产生数字资产的权属纠纷时,能够为数字资产的合法持有者进行有效确权。

附图说明

[0012] 为了更清楚地说明本发明实施例的技术方案,以下对本发明实施例中的附图作简单介绍。

[0013] 图1是根据本发明一个实施例的数字资产处理流程图。

[0014] 图2是根据本发明一个实施例的在数字资产上链前基于抗量子密钥的数字资产处理方法流程图。

[0015] 图3是根据本发明另一个实施例的在数字资产上链前基于抗量子密钥的数字资产处理方法流程图。

[0016] 图4是根据本发明一个实施例在数字资产确权时基于抗量子密钥的数字资产处理方法流程图。

[0017] 图5是根据本发明一个实施例的基于抗量子密钥的第一数字资产处理装置原理框图。

[0018] 图6是根据本发明一个实施例的基于抗量子密钥的第二数字资产处理装置原理框图。

[0019] 图7是根据本发明应用基于抗量子密钥的数字资产处理装置的系统框图。

[0020] 图8是根据本发明应用基于抗量子密钥的数字资产处理装置的另一系统框图。

[0021] 图9是根据本发明一个实施例的电子设备的硬件结构原理示意图。

具体实施方式

[0022] 以下将参考若干示例性实施方式来描述本发明的原理和精神。应当理解,提供这些实施方式的目的是为了使本发明的原理和精神更加清楚和透彻,使本领域技术人员能够更好地理解进而实现本发明的原理和精神。本文中提供的示例性实施方式仅是本发明的一部分实施方式,而不是全部的实施方式。基于本文中的实施方式,本领域普通技术人员在不付出创造性劳动前提下所获得的所有其他实施方式,都属于本发明保护的范围。

[0023] 本发明提供了一种数字资产版权保护处理方法、装置、电子设备、存储介质及计算机程序产品,用以保护数字资产版权,解决数字资产确权难度大的问题。

[0024] 图1是根据本发明一个实施例的数字资产处理流程图。在本实施例中,首先在数字资产生成后或生成的过程中对其进行签名处理,并将数字签名及签名过程中产生的确权时需要的数据(以下简称确权基础数据)存储在公信数据库,而后再将签名处理后的数字资产发布到区块链上形成共识。区块链或者为签约区块链,如Opensea;区块链或者为以太坊公链,如元镜MetaMirror;区块链又或者为联盟链,如NFT中国;当然也可以是其他一些区块链,如鲸探等等。上链后的数字资产如现有其他的数字资产一样在链上展示,并按照规定的交易处理方式进行自由交易。在交易过程中,除了按照现有的数字资产交易模式进行交易之外,由于本发明中的数字资产在上链之前进行了签名等特定处理,具有数字签名、公钥及其他一些确权时需要使用的数据,因而在交易过程中数字资产的原持有人还需将确权基础数据连同数字资产一并转移给交易方,从而使该交易方成为数字资产新的原持有人,并同时持有相应的确权基础数据。

[0025] 当在数字资产的展示过程中或交易后出现被盗版情况时,即发生了权属纠纷问题,通过本发明提供的方法对数字资产进行相关处理则可以确定当前数字资产的持有人是否为真正的持有人。

[0026] 图2是根据本发明一个实施例的在数字资产上链前基于抗量子密钥的数字资产处理方法流程图,本实施例的数字资产加密处理方法具体包括以下步骤。

[0027] 步骤S11,生成预置位数的随机数,基于随机数采用抗量子密钥算法生成一对私钥和公钥。

[0028] 步骤S12,将记录有数字资产归属权的确权信息加密为密文。

[0029] 步骤S13,将密文和随机数混合拼接在一起得到中间信息。

[0030] 步骤S14,将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中。

[0031] 步骤S15,采用抗量子密钥算法生成的私钥对隐写后的多媒体文件进行签名处理以生成隐写后的多媒体文件的数字签名。

[0032] 步骤S16,发布经过签名处理的隐写后的多媒体文件。

[0033] 在步骤S11中,通过随机数函数生成一个具有指定位数的随机数,如128位或256位的随机数。为了防止采用量子破解的方式破解本发明中使用的密钥,本发明采用抗量子密钥算法基于该随机数生成一对私钥和公钥。作为示例,可采用但不限于基于多变量(Multivariate-based) 的算法、基于格 (Lattice-based)的算法,基于编码 (Code-based) 的算法或基于哈希 (Hash-based) 的算法中的至少一种。

[0034] 以基于多变量 (Multivariate-based) 的算法为例,对公钥和私钥的生成原理及过程简要说明如下。

[0035] 首先构造含有q个元素的有限域k和一组(m个)有限域k上的d次n元多项式 $F_q[x_1,\cdots,x_n]$,在本实施例中,以二次n元多项式为例,二次n元多项式如下式所示。

[0036]
$$\begin{aligned} f_1(x_1,\cdots,x_n) &= \sum_{1\le i,j\le n} a_{i,j}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d^{(1)} \\ f_2(x_1,\cdots,x_n) &= \sum_{1\le i,j\le n} a_{i,j}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d^{(2)} \\ &\vdots \\ f_m(x_1,\cdots,x_n) &= \sum_{1\le i,j\le n} a_{i,j}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d^{(m)} \end{aligned}$$

[0037] 上式中的 $X_1,\ldots,X_n$ 为n个变量。

[0038] $a_{i,j}^{(1)}\ldots\ldots a_{i,j}^{(m)}$ 和 $b_i^{(1)}\ldots\ldots b_i^{(m)}$ 为多项式系数,$c^{(1)}\ldots\ldots c^{(m)}$ 为多项式常量,其数值为通过随机数函数生成的随机数。

[0039] 而后进行多项式映射F:$\mathbb{F}_q^n \to \mathbb{F}_q^m$。

[0040] 即 $F_q[x_1,\cdots,x_n]=(f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n))$ 。

[0041] 其中每一个 $f_i \in F_q[x_1,\cdots,x_n]$ 是二次多项式。

[0042] 这里的F须满足F的原像在计算上能够找到且可逆这一条件。

[0043] 而后分别对前述的两个多项式 $\mathbb{F}_q^n$ 和 $\mathbb{F}_q^m$ 进行随机可逆的线性映射,该线性映射可表示如下。

[0044] S: $\mathbb{F}_q^m \to \mathbb{F}_q^m$ 和T:$\mathbb{F}_q^n \to \mathbb{F}_q^n$

[0045] 在本实施例中,公钥为P=S*F*T,*表示变换的复合。

[0046] 其中, P可以表示为下式。

[0047] $$P(x_1,\cdots,x_n)=(p_1(x_1,\cdots,x_n),\cdots,p_m(x_1,\cdots,x_n)) \quad (1-1)$$

[0048] 私钥为三次映射计算：S、T和F。

[0049] 其他三种抗量子密钥算法生成密钥的过程可参考各自的算法指南来实现，在此不再赘述。

[0050] 在步骤S12中，确权信息例如为当前数字资产持有人设定的一个特定内容，其表现形式可以是文本、图片、音频或视频，也可是对记录有特定内容的文本、图片、音频或视频进行哈希计算后得到的数字摘要。特定内容代表数字资产的归属权。例如，当前数字资产持有人可以写下长短任意的一段文字，可以录下任意声音的一段音频，可是任意的一张照片，还可以是一段视频。进一步地，还可以对这些文本、图片、音频或视频按照摘要算法(如MD5、SHA-1或SHA-256)进行处理得到数字摘要。而后采用任意一种加密算法对当前的文本文件、图片文件、音频文件视频文件或数字摘要加密得到密文。加密算法需为可逆算法，即可解密得到原始信息。如对称式加密算法，如DES、3DES或AES系列算法，或者一些非对称式加密算法，如RSA，ECC椭圆曲线加密相关算法等等，在此不再赘述。

[0051] 为了提高对密文的破解难度，也可以采用抗量子加密算法对原始确权信息进行加密。如按照前述步骤S11中的方法生成另一对公钥和私钥，例如，公钥为$P_1=S_1*F_1*T_1$，*表示变换的复合，私钥为三次映射计算S_1、T_1和F_1。

[0052] 采用公钥P_1对记录有数字资产归属权的确权信息进行加密，即需要按照公式(1-1)计算$P_1(r)=w$，其中的r为要被加密的文件，即确权信息；w为加密后的密文。

[0053] 为了后续的确权需要，将数字资产持有人设定的特定内容嵌入到数字资产中，为了提高获得数字资产持有人设定的特定内容的难度，本发明在对数字资产持有人设定的特定内容加密后，在步骤S13，将密文和生成的预置位数的随机数混合拼接在一起得到一个中间信息，而后在步骤S14，将中间信息以隐写的方式嵌入作为数字资产表现形式的多媒体文件中。

[0054] 为了进一步提高从中间信息中获得密文的难度，本发明提供有多种混合拼接处理方式，混合拼接处理方式的选择可由拼接参数k的值确定。在一个实施例中，拼接参数k的值对应混合拼接处理方式的序号。当混合拼接处理方式有n种时，拼接参数k的取值范围为[1,……,n]，在理论上，n可以为无穷大。

[0055] 本发明在密文混合拼接的时候随机抽取一种混合拼接处理方式进行密文拼接，总的抽取方法有$C_n^1+C_n^2+C_n^3+\ldots\ldots+C_n^n=2^n-1$ 种，因而破解中间信息获得密文的复杂度为 $O(2^n-1)$，属于NP-hard问题，因而难以破解。由于每次对一个数字资产的确权信息进行加密处理时，对密文和随机数进行拼接时使用的混合拼接处理方式都不同，即使从一个数字资产中破解出中间信息，但也很难从其他数字资产中破解出中间信息。

[0056] 在一个关于混合拼接处理的实施例中，首先将密文的每个字符转换成16进制，而后在每个16进制的密文字符后插入一个随机字符。在另一个关于混合拼接处理的实施例中，将随机字符按照逆序的方式插入到正序的16进制密文字符后。在又一个关于混合拼接处理的实施例中，将随机数的每个字符也转换为16进制数，在向密文中插入16进制的随机字符后进行计算，如将每一个相邻的16进制的密文字符和16进制的随机字符做加、减、乘或除等运算，再将运算结果插入当前的位置，也可以由运算结果替换相邻的16进制的密文字

符和16进制的随机字符。

[0057] 前述的几个混合拼接处理方式仅仅是示意性的,本领域的普通技人员可知,在向密文中插入随机字符时,通过设定不同的插入位置、每次插入的随机字符数量、计算处理方式、计算结果的处理方式等等可以变换得到n个混合拼接处理方式, 在此不再赘述。

[0058] 在步骤S14中,在向作为数字资产表现形式的多媒体文件中隐写中间信息时,隐写处理方式同样有多种,其选择方法与混合拼接处理方式的选择方法相同,即随机指定本次隐写时对应的隐写参数j的值,基于隐写参数j的值确定对应的隐写处理方式。在本实施例中,数字资产表现形式可以是图片、音频或视频。以图片为例,在向图片中隐写中间信息时,隐写处理方式如下。

[0059] 首先,将中间信息转换为二进制。

[0060] 而后,读取图片中每一个像素的RGB三个通道值,并将RGB通道值分别转换为二进制,即得到每一个像素得到R通道二进制值、G通道二进制值和B通道二进制值。

[0061] 最后,依据二进制的中间信息,改变每一个像素的三个通道二进制值中的最后一位。在一个实施例中,可按照中间信息中二进制数的顺序,依次对每一个像素的RGB三个通道的最后一位加/减0或1。在另一实施例中,可将中间信息中二进制数与每一个像素的RGB三个通道的最后一位相加的结果替换原通道的最后一位。通过改变计算时使用的算法、改变计算时所用的中间信息中二进制数的数量、改变选取的像素值中可替换的RGB三个通道中的任意一个或多个通道、改变选取的像素等等可以衍生出多种隐写处理方式。为了确定每次隐写时使用的隐写处理方式,本发明设置有隐写参数j,每个隐写参数j的值对应一个隐写处理方式,隐写参数j的值可以随机确定。

[0062] 当数字资产表现形式为音频文件时,同样可以采用前述与图片的隐写处理方式相同的方法进行隐写,不同在于,首先获取音频文件的时域波形的16位采样点值,而后再改变16位采样点值的最后一位,改变值的方法可以按前述向图片隐写时所使用的隐写处理方法。另外,音频的隐写方法还有很多,例如回声隐藏法、相位编码法、扩频法等等,在此不再一一赘述。

[0063] 当数字资产表现形式为视频时,可将其视为图片与音频的结合体,因而可以采用前述的对图片隐写的方法、对音频隐写的方法或者二者结合得到的方法对视频进行隐写,对应的隐写处理方式相对于单独的对图片或音频隐写时的处理方式更多,因而破解难度也就更大。

[0064] 在隐写完成后,在步骤S15采用步骤S11中抗量子密钥算法生成的私钥对隐写后的多媒体文件进行签名处理得到隐写后的多媒体文件的数字签名。具体过程如下。

[0065] 首先计算隐写后的多媒体文件的数字摘要,采用的算法例如MD5、SHA-1或SHA-256等算法。

[0066] 而后按照下式对数字摘要依次按照S、T好F进行三次映射计算。

$$S^{-1}(m)=y \quad (2\text{-}1)$$

[0067]

$$F^{-1}(y)=z \quad (2\text{-}2)$$

$$T^{-1}(z)=x \quad (2\text{-}3)$$

[0068] 其中,m为隐写后的多媒体文件的数字摘要,x为隐写后的多媒体文件的数字签名。

[0069] 隐写后的多媒体文件的数字签名和对应的公钥P可以填加到隐写后的多媒体文件中,如填加在图片、音频文件、视频文件的尾部,也可以存储于公信数据库。同时,建立数字签名验证用的公钥、确权信息、对加密的确权信息进行解密的私钥、混合拼接处理方式、隐写处理方式与上链的新多媒体文件的关联关系,并将签名验证用的公钥、确权信息、对加密的原始确权信息进行解密的私钥、混合拼接处理方式、隐写处理方式作为确权基础数据存储于公信数据库,以便在确权时使用。

[0070] 在本实施例中,在对数字资产进行签名处理的过程中,在数字资产中嵌入了可以证明该数字资产归属权的内容,为了保护该内容不被持有人之外的人获得,本实施例首先对可以证明该数字资产归属权的内容进行加密得到密文,再拼接一个随机数后以隐写的方式嵌入数字资产中,再针对隐写后数字资产进行签名。若要伪造签名,首先要破解抗量子密钥算法本身,而后再按照破解后的抗量子密钥算法得到签名的私钥,然后还需要正确反隐写以得到隐写的中间信息,并需要从中间信息中正确拆分出密文,最后还需要对密文进行破解。本实施例在拼接中间信息、隐写等每个流程都构造了一个NP-hard问题,再加上抗量子密钥算法目前也是Shor算法所无法破解的,从而使得对应用本实施例签名处理得到的数字资产进行破解时的复杂度极高,在目前有限条件下和未来量子计算机成熟后都具有不可破解性。

[0071] 图3是根据本发明另一个实施例在数字资产上链前基于抗量子密钥的数字资产处理方法流程图,本实施例的基于抗量子密钥的数字资产处理方法具体包括以下步骤。

[0072] 步骤S21,生成预置位数的随机数,基于随机数采用抗量子密钥算法生成一对私钥和公钥。

[0073] 步骤S22,将记录有数字资产归属权的确权信息加密为密文。

[0074] 步骤S23,将密文和生成的预置位数的随机数混合拼接在一起得到中间信息。

[0075] 步骤S24,将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中。

[0076] 步骤S25,采用抗量子密钥算法生成的私钥对隐写后的多媒体文件进行签名处理得到隐写后的多媒体文件的数字签名。

[0077] 步骤S26,将经过签名处理的隐写后的多媒体文件拼接在作为数字资产的多媒体文件数据后。

[0078] 步骤S27,扰乱拼接处的数据块,该数据块包括作为数字资产的多媒体文件尾部的部分数据块和经过签名处理的隐写后的多媒体文件头部的部分数据块。

[0079] 步骤S28,发布拼接在作为数字资产的多媒体文件数据后且拼接处的数据块被扰乱的经过签名处理的隐写后的多媒体文件,即发布拼接后的文件。

[0080] 其中,在步骤S21至步骤S25的处理过程与前述图2中的步骤S11至步骤S15的处理过程相同,在此不再赘述。步骤S25中生成的数字签名可以填加到隐写后的多媒体文件中或存储于公信数据库;验证数字签名用的公钥也可以存储于公信数据库。

[0081] 在步骤S26中将经过签名处理的隐写后的多媒体文件拼接在作为数字资产的多媒体文件(或称为原多媒体文件)数据后得到了一个新的文件,而后在步骤S27中在拼接处获取的一定数据量的数据块,该数据块包括原多媒体文件尾部的一定字节量的数据,如16个字节的数据,该数据块还包括经过签名处理后的隐写后的多媒体文件头部中的一定字节量

的数据,如也是16个字节的数据,当然也可以是8个、12个、24个等。也就是说,获取的数据块由原多媒体文件尾部的部分数据和隐写后的多媒体文件头部的部分数据构成。在另一个实施例中,数据块中原多媒体文件尾部的16个字节数据可以是连续的数据,也可以是间隔的数据,数据块中隐写后的多媒体文件头部的数据可以是连续的数据,也可以是间隔的数据。

[0082] 其中,不同类型文件的文件头标识固定且不同,例如,PNG格式的文件头标识为89504E47,又例如,GIF格式的文件头标识为47494638 ,AVI 格式的文件头标识为41564920,Wave (wav)格式的文件头标识为57415645,因而,为了获取到两个文件拼接处的数据块,在一个实施例中,首先从拼接后的文件头部开始遍历数据以查找隐写后的多媒体文件头标识,当找到了隐写后的多媒体文件头标识,也得到了原多媒体文件的尾部,即准确定位到了拼接位置,而后再按照前述方式得到包括两个文件数据的数据块。

[0083] 在步骤S27中,扰乱两个文件拼接处的数据块,以此进一步增强密文的获取难度。在一个实施方式中,可以互换原多媒体文件尾部数据和隐写后的多媒体文件头部的数据,确定互换位置的方法可以有多种。如从连接的地方开始两两互换,或者都按从前向后的顺序互换,或者按照尾部数据的位置为自变量a,头部数据的位置为变量b,构建自变量a与变量b的函数,按照该函数进行位置互换,函数例如为一次函数,如:b=a+1,b=a+2等等。在另一个实施方式中,以向当前数据块内增加其他数据的方式以扰乱拼接文件的拼接痕迹。在一个实施例中,生成一个随机数,将随机数插入到当前的数据块中,通过改变随机数的位数、插入位置、一个插入位置可以插入的字符数量,该方式也有多种方法。综上,前述实施例中的每种扰乱拼接文件的拼接处的数据块的方法均为扰乱处理方式中的一种,以扰乱参数p的值来对应一种扰乱处理方式,扰乱参数p的值的取值范围为[1,……,n], n为第n个扰乱处理方式的序号。在步骤S27中通过扰乱参数p的值来确定扰乱处理方式,扰乱参数p的值可随机在1-n中指定。同理,当使用了扰乱处理方式后,将当前使用的扰乱处理方式也作为一种确权基础数据存储到公信数据库。

[0084] 在本实施例中,在对数字资产表现形式的多媒体文件完成隐写后,为了防止被识别出经过隐写处理,将原多媒体文件数据拼接到经过隐写的多媒体文件数据之前,从而使得在链上展示时展示的仍然是原多媒体文件,避免他人通过机器学习等方法识别出展示的文件为经过隐写处理的多媒体文件。

[0085] 在另一个实施例中,按照前述实施例步骤S21至步骤S24得到隐写后的多媒体文件后,将原多媒体文件拼接在隐写后的新的多媒体文件后,而后再对拼接后的文件进行数字签名,则进一步提高了伪造数字签名的难度。

[0086] 在另一个实施例中对步骤S23中得到的中间信息进行签名处理。而后再进行隐写处理,还可以将原多媒体文件拼接在隐写后的新的多媒体文件后。相关处理过程可参考前述实施例, 在此不再赘述。

[0087] 多媒体文件在上链展示的过程中和交易后,由于数字资产的表现形式为图片、音频、视频等,很容易被模仿而发生盗版的情况。在必要时候可以通过确权处理来对争议数字资产进行权属鉴别和认证。由于现有技术中作为数字资产的多媒体文件在创建时并没有经过特定处理,不能从多媒体文件本身进行确权,因而确权非常困难。当采用本发明提供的处理方法在多媒体文件上链前进行处理后,在确权时通过对多媒体文件本身进行的处理则可以对争议数字资产进行权属鉴别和认证。

[0088] 图4是根据本发明一个实施例在数字资产确权时基于抗量子密钥的数字资产处理方法流程图。本实施例的数字资产处理方法具体包括以下步骤。

[0089] 步骤S31,获取待确权的多媒体文件的数字签名,并采用抗量子密钥算法生成的公钥对待确权的多媒体文件的数字签名进行验证。

[0090] 步骤S32,判断对数字签名的验证是否通过,如果验证通过,则在步骤S33对待确权的多媒体文件进行反隐写处理。如果验证没有通过,则在步骤S42确定待确权的多媒体文件没有通过归属权确权,即待确权的多媒体文件不是持有人声称的合法数字资产。

[0091] 步骤S34,判断反隐写处理后是否得到中间信息,如果没有得到中间信息,则在步骤S42确定待确权的多媒体文件没有通过归属权确权。如果反隐写处理后得到了中间信息,则在步骤S35对该中间信息进行拆分处理。

[0092] 步骤S36,判断是否从中间信息中拆分出密文,如果没有从该中间信息中拆分出密文,则在步骤S42确定待确权的多媒体文件没有通过归属权确权。如果从该中间信息中拆分出密文,则在步骤37对密文进行解密。

[0093] 步骤S38,判断是否解密到了用于确权的信息,如果没有解密出用于确权的信息,则在步骤S42确定待确权的多媒体文件没有通过归属权确权。如果解密出用于确权的信息,则在步骤S39将解密到的用于确权的信息与待确权的多媒体文件所对应的数字资产归属权(即真正的确权信息)进行对比。

[0094] 步骤S40,判断二者是否一致,如果二者一致,则在步骤S41,确定待确权的多媒体文件通过归属权确权,如果二者不一致,在步骤S42确定待确权的多媒体文件没有通过归属权确权。

[0095] 其中,采用抗量子密钥算法生成的与签名验证时使用的公钥相应的私钥被配置为在发布待确权的多媒体文件时生成待确权的多媒体文件的数字签名。

[0096] 对于一个合法来源的数字资产,在交易时新持有人除了从原持有人处获得多媒体文件外,还包括该多媒体文件的确权基础数据。因而在确权时,根据新持有人提供的待确权多媒体文件,可以从公信数据库中获得与之对应的确权基础数据,确权基础数包括了记录数字资产归属权的确权信息及其解密用的私钥、混合拼接密文与随机数时使用的混合拼接处理方式(例如拼接参数k的值)、隐写处理方式(例如隐写参数j的值)、数字签名及验证数字签名用的公钥等。当采用原多媒体文件拼接隐写后的多媒体文件时,还包括扰乱文件数据拼接处数据时使用的扰乱处理方式(例如扰乱参数p的值)。因而当已知一个待确权的多媒体文件时,对于一个合法的多媒体文件,其必然包括前述的确权基础数据,在进行确权处理过程中,依据处理需求从确权基础数据中读取所需要的数据进行处理。

[0097] 在步骤S31中采用对应的数字签名验证用的公钥对数字签名进行验证时,首先采用确权基础数据中的用于验证数字签名的公钥对数字签名x进行计算得到一个数字摘要m_1,而后计算待确权的多媒体文件的另一个数字摘要m_2,而后对比两份数字摘要是否一致;当两份数字摘要一致,确定对数字签名的验证通过,当两份数字摘要不一致,确定对数字签名的验证没有通过。其中,在对数字签名x进行计算时,按照抗量子密钥算法得到的公钥P对数字签名进行计算,即计算P(x),其中,x为数字签名,经过 P(x)计算后得到数字摘要m_1。当签名处理的文件为中间信息时,在确权处理时,在反隐写处理得到中间信息时,计算中间信息的数字摘要,用来与经P(x)计算后得到数字摘要m_1进行对比。当待确权的多媒体文件是

拼接文件时,在确权处理时,在从待确权的多媒体文件提取到隐写后的多媒体文件时,计算隐写后的多媒体文件的数字摘要,用来与经P(x)计算后得到数字摘要m_1进行对比。

[0098] 在步骤33中对待确权的多媒体文件进行反隐写处理时,从确权基础数据中读取隐写参数j的值,根据隐写参数j的值确定与其对应的隐写处理方式,按照对应该隐写处理方式相反的步骤进行反隐写。

[0099] 在步骤S35中对中间信息进行拆分处理时,首先从确权基础数据中读取混合拼接处理方式拼接参数k的值,根据拼接参数k的值确定与其对应的混合拼接处理方式,再根据混合拼接处理方式逐一从中间信息中拆分出密文与随机数等等。

[0100] 在步骤37中采用私钥对密文进行解密时,当加密时采用的是DES、3DES或AES系列算法或者一些非对称式加密算法(如RSA,ECC椭圆曲线加密相关算法)时,采用对应的私钥进行解密。如果加密时使用的公钥采用的是通过基于多变量 (Multivariate-based) 的算法生成时,解密时使用的私钥为三次映射计算S、T和F。因而解密的过程分别为三次映射计算S、 T和F。

[0101] 如果确权基础数中包含了扰乱参数p值,则首先按照与扰乱参数p值对应的扰乱处理方式恢复待确权的多媒体文件中的拼接处的数据;接着从拼接处的数据中的头部数据向后提取出隐写后的多媒体文件;然后再对提取出的隐写后的多媒体文件进行反隐写、拆分、解密、签名验证等处理。

[0102] 如果在数字签名验证、恢复拼接处的数据、反隐写、拆分、解密、确权信息对比的处理过程中的任意一个步骤出现问题都可以确定当前待确权的多媒体文件与上链的多媒体文件不一致,因而不能证明待确权的多媒体文件的现持有人是该多媒体文件的合法持有人。

[0103] 在另一方面,本发明还提供了基于抗量子密钥的数字资产处理装置。

[0104] 图5是根据本发明一个实施例的基于抗量子密钥的第一数字资产处理装置原理框图。如图5所示,本实施例中的第一数字资产处理装置10包括密钥单元11、加密单元12、拼接单元13、隐写单元14、签名单元15和发布单元16。

[0105] 其中,密钥单元11被配置为生成预置位数的随机数,并基于随机数采用抗量子密钥算法生成一对用于进行签名的第一私钥和第一公钥,其中,第一私钥和第一公钥分别被配置为进行数字签名处理及在对发布的多媒体文件确权时对数字签名进行验证。密钥单元11基于任意一种加密算法生成用于加密的一对第二私钥和第二公钥。加密算法可以为DES、3DES或AES系列的对称式加密算法,也可以为RSA或ECC椭圆曲线等非对称式加密算法,还可以为基于格 (Lattice-based)的算法、基于编码 (Code-based) 的算法、基于多变量 (Multivariate-based) 的算法或基于哈希 (Hash-based) 的算法等抗量子密钥算法。例如生成另一个随机数,基于该随机数采用基于多变量 (Multivariate-based) 的算法生成用于加密的第二私钥和第二公钥,随机数位数例如为256位。第二公钥和第二私钥分别被配置为对记录有数字资产归属权的确权信息进行加密和在对发布的多媒体文件确权时对从反隐写得到的中间信息中拆分出的密文进行解密。

[0106] 加密单元12采用加密用的第二公钥将记录有数字资产归属权的确权信息加密为密文。确权信息可以为当前数字资产持有人设定的一个特定内容,特定内容代表数字资产的归属权,其表现形式可以是文本、图片、音频或视频,也可以是对记录有特定内容的文本、

图片、音频或视频进行哈希计算后得到的数字摘要。

[0107] 拼接单元13将密文和随机数混合拼接在一起得到中间信息。作为示例,拼接单元13可通过随机指定拼接参数k的值确定一个混合拼接处理方式,将加密单元12生成的密文和密钥单元11生成的随机数混合拼接在一起得到中间信息。

[0108] 隐写单元14将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中。作为示例,隐写单元14可通过随机指定的隐写参数j的值确定隐写处理方式,将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中。

[0109] 签名单元15采用第一私钥对隐写后的多媒体文件进行签名处理得到隐写后的多媒体文件的数字签名;或者,签名单元15采用第一私钥对中间信息进行签名处理得到数字签名。生成的数字签名可以填加到隐写后的多媒体文件中或存储到公信数据库中。

[0110] 发布单元16发布经过签名处理的隐写后的多媒体文件。

[0111] 在另一个实施例中,第一数字资产处理装置10还可以包括文件拼接单元17,如图中的虚线所示,其用于将隐写后的多媒体文件数据拼接在作为数字资产的多媒体文件(或称为原多媒体文件)数据后,然后按照扰乱处理方式扰乱两个文件拼接处的数据块。在该实施例中,发布单元16发布拼接在作为数字资产的多媒体文件数据后且拼接处的数据块被扰乱的隐写后的多媒体文件。又或者,签名单元15对拼接在作为数字资产的多媒体文件数据后且拼接处的数据块被扰乱的隐写后的多媒体文件进行签名处理,发布单元16发布经过签名处理的拼接在作为数字资产的多媒体文件数据后且拼接处的数据块被扰乱的隐写后的多媒体文件。

[0112] 图6是根据本发明一个实施例的基于抗量子密钥的第二数字资产处理装置原理框图。如图6所示,本实施例中的第二数字资产处理装置20包括签名验证单元21、反隐写单元22、拆分单元23、解密单元24和对比单元25和确权单元26。

[0113] 签名验证单元21被配置为采用抗量子密钥算法生成的公钥对待确权的多媒体文件的数字签名进行验证。其中,在进行数字签名验证时,在对待确权的多媒体文件在发布前进行的处理时,如果在对待确权的多媒体文件进行发布前的处理时是对隐写后的多媒体文件进行的签名,签名验证单元21首先采用确权基础数据中的用于验证数字签名的公钥对数字签名x进行计算得到一个数字摘要m_1,而后计算待确权的多媒体文件得到另一个数字摘要m_2,而后对比两份数字摘要是否一致;当两份数字摘要一致,确定对数字签名的验证通过,当两份数字摘要不一致,确定对数字签名的验证没有通过。其中,在对数字签名x进行计算时,按照抗量子密钥算法得到的公钥P对数字签名进行计算,即计算P(x),其中,x为数字签名,经过 P(x)计算后得到数字摘要m_1。

[0114] 如果在对待确权的多媒体文件进行发布前的处理时是对密文和随机数混合拼接构成的中间信息加密时,先由反隐写单元22按照隐写处理方式进行反隐写处理,在得到中间信息时,对中间信息计算得到数字摘要m_3,对比对数字签名x进行计算得到的数字摘要m_1和对中间信息计算得到数字摘要m_3是否一致,当两份数字摘要一致,确定对数字签名的验证通过,当两份数字摘要不一致,确定对数字签名的验证没有通过。

[0115] 反隐写单元22对待确权的多媒体文件进行反隐写处理。拆分单元23响应于对待确权的多媒体文件进行反隐写处理得到中间信息而对中间信息进行拆分处理。解密单元24响应于对中间信息进行拆分处理得到密文而采用私钥对密文进行解密。对比单元25响应于对

密文进行解密得到确权信息,将解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权进行对比。确权单元26响应于解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权一致,确定待确权的多媒体文件通过归属权确权,确权单元26响应于待确权的多媒体文件的数字签名没有通过验证,或者对待确权的多媒体文件进行反隐写处理没有得到中间信息,或者对中间信息进行拆分处理没有得到密文,或者对密文进行解密没有得到确权信息,或者在解密得到的确权信息与待确权的多媒体文件所对应的数字资产归属权不一致时,确定待确权的多媒体文件没有通过归属权确权。

[0116] 在另一个实施例中,第二数字资产处理装置20还包括文件提取单元27,如图6中的虚线所示。当确权基础数中包含了扰乱参数p值,文件提取单元27首先按照扰乱参数p值对应的扰乱处理方式恢复待确权的多媒体文件中作为数字资产的多媒体文件和隐写后的多媒体文件拼接处的数据;然后基于拼接处的数据中的文件头部数据向后提取出隐写后的多媒体文件,并将其发送给反隐写单元22,反隐写单元22对提取出的隐写后的多媒体文件进行反隐写处理。当文件提取单元27提取文件失败时发送通知给确权单元26,确权单元26可确定对待确权的多媒体文件没有通过归属权确权。如果待确权的多媒体文件在发布前对隐写后的多媒体文件进行了签名,当隐写后的多媒体文件数据拼接在作为数字资产的多媒体文件数据后时,文件提取单元27将提取出的隐写后的多媒体文件发送给签名验证单元21。签名验证单元21以提取出的隐写后的多媒体文件为处理对象进行签名验证。

[0117] 第一数字资产处理装置10和第二数字资产处理装置20可以设置在同一个系统中,也可以分置于不同系统中。

[0118] 图7是根据本发明应用基于抗量子密钥的数字资产处理装置的系统框图。

[0119] 如图7所示,第一数字资产创建系统101包括第一数字资产处理装置10和数字资产内容创建装置100,数字资产内容创建装置100创建作为数字资产的多媒体文件,第一数字资产处理装置10对创建完成的多媒体文件进行处理,如设置记录有数字资产归属权的确权信息并对其进行加密;基于随机数采用抗量子密钥算法生成一对私钥和公钥;将密文和随机数混合拼接在一起得到中间信息;将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中;采用私钥对隐写后的多媒体文件进行签名处理得到数字签名,并将处理过程中的确权基础数据存储到公信数据库300中,而后再将经过处理的多媒体文件发布到区块链400上。用于对数字资产进行确权的第二数字资产处理装置20位于第一平台201中,当需要对作为数字资产的多媒体文件确权时,由第一平台201中的第二数字资产处理装置20对待确权的多媒体文件进行确权处理。具体的确权处理参见前述说明,在此不再赘述。另外,确权处理中所需要的确权基础数据也可以由待确权的多媒体文件的持有人提供。

[0120] 图8是根据本发明应用基于抗量子密钥的数字资产处理装置的另一系统框图。

[0121] 如图8所示,第一数字资产处理装置10和第二数字资产处理装置20均位于第二平台202中。第二数字资产创建系统102包括数字资产内容创建装置100,数字资产内容创建装置100创建作为数字资产的多媒体文件,在需要发布到区块链400上时,第二数字资产创建系统102将数字资产内容创建装置100创建完成的作为数字资产的多媒体文件发送给第二平台202,由第一数字资产处理装置10进行加密、拼接、隐写和签名等处理,在处理完成后发布到区块链400,并将处理过程中产生的确权基础数据存储到公信数据库300中。当需要确权时,由第二方平台202中的第二数字资产处理装置20对待确权的多媒体文件进行确权处

理,确权处理中所需要的确权基础数据由公信数据库300提供或对待确权的多媒体文件持有人提供。

[0122] 在另一方面,本发明还提供一种电子设备,包括处理器以及存储有计算机程序指令的存储器;电子设备执行计算机程序指令时实现前述的基于抗量子密钥的数字资产处理方法。

[0123] 图9是根据本发明一个实施例的电子设备的硬件结构原理示意图。如图9所示,电子设备可以包括处理器601以及存储有计算机程序指令的存储器602。

[0124] 具体地,上述处理器601可以包括中央处理器(CPU),或者特定集成电路(Application Specific Integrated Circuit ,ASIC),或者可以被配置成实施本发明实施例的一个或多个集成电路。

[0125] 存储器602可以包括用于数据或指令的大容量存储器。举例来说而非限制,存储器602可包括硬盘驱动器(Hard Disk Drive,HDD)、软盘驱动器、闪存、光盘、磁光盘、磁带或通用串行总线(Universal Serial Bus,USB)驱动器或者两个或更多个以上这些的组合。在合适的情况下,存储器602可包括可移除或不可移除(或固定)的介质。在合适的情况下,存储器602可在综合网关容灾设备的内部或外部。在特定实施例中,存储器602是非易失性固态存储器。

[0126] 在一个示例中,电子设备还可包括通信接口603和总线610。其中,如图9所示,处理器601、存储器602、通信接口603通过总线610连接并完成相互间的通信。通信接口603主要用于实现本发明实施例中各模块、装置、单元和/或设备之间的通信。总线610包括硬件、软件或两者,将在线数据流量计费设备的部件彼此耦接在一起。举例来说而非限制,总线可包括加速图形端口(AGP)或其他图形总线、增强工业标准架构(EISA)总线、前端总线(FSB)、超传输(HT)互连、工业标准架构(ISA)总线、无限带宽互连、低引脚数(LPC)总线、存储器总线、微信道架构(MCA)总线、外围组件互连(PCI)总线、PCI-Express(PCI-X)总线、串行高级技术附件(SATA)总线、视频电子标准协会局部(VLB)总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下,总线610可包括一个或多个总线。尽管本发明实施例描述和示出了特定的总线,但本发明考虑任何合适的总线或互连。

[0127] 处理器601通过读取并执行存储器602中存储的计算机程序指令,实现上述基于抗量子密钥的数字资产处理方法。

[0128] 本发明实施例中的电子设备可以是服务器、个人电脑或其他形式的计算设备。

[0129] 另一方面,本发明实施例还提供了计算机可读存储介质,计算机存储介质上存储有计算机程序指令,计算机程序指令被处理器执行时实现上述基于抗量子密钥的数字资产处理方法。

[0130] 另一方面,本发明实施例提供了计算机程序产品,其包括计算机程序指令,计算机程序指令被处理器执行时实现上述基于抗量子密钥的数字资产处理方法。计算机程序产品例如为应用安装包、插件等。

[0131] 以上所述,仅为本发明的具体实施方式,所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,上述描述的系统、模块和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。应理解,本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到各种等效的修改或替换,

这些修改或替换都应涵盖在本发明的保护范围之内。

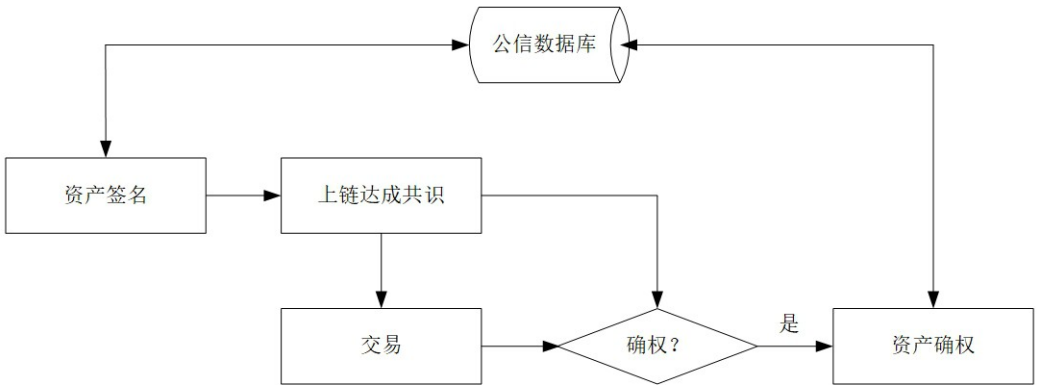

公信数据库
资产签名
上链达成共识
交易
确权？
是
资产确权

图 1

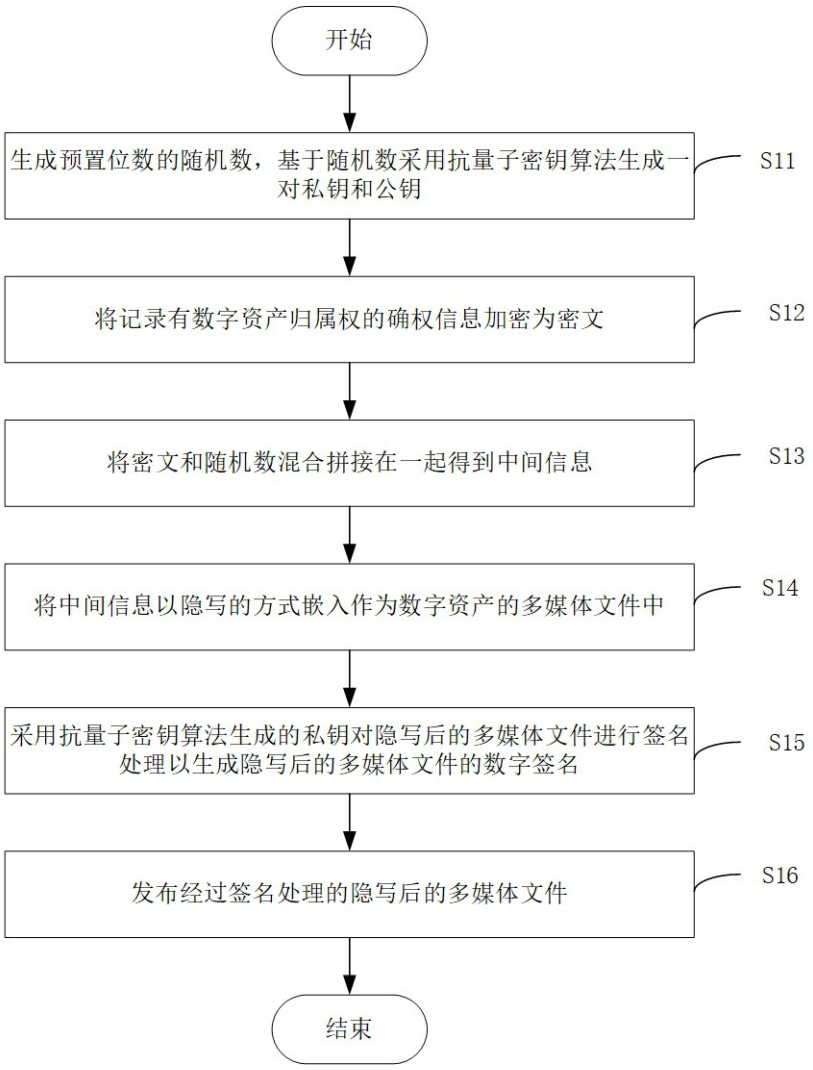

开始
生成预置位数的随机数，基于随机数采用抗量子密钥算法生成一对私钥和公钥
S11
将记录有数字资产归属权的确权信息加密为密文
S12
将密文和随机数混合拼接在一起得到中间信息
S13
将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中
S14
采用抗量子密钥算法生成的私钥对隐写后的多媒体文件进行签名处理以生成隐写后的多媒体文件的数字签名
S15
发布经过签名处理的隐写后的多媒体文件
S16
结束

图 2


开始
生成预置位数的随机数，基于随机数采用抗量子密钥算法生成一对私钥和公钥
S21
将记录有数字资产归属权的确权信息加密为密文
S22
将密文和随机数混合拼接在一起得到中间信息
S23
将中间信息以隐写的方式嵌入作为数字资产的多媒体文件中
S24
采用抗量子密钥算法生成的私钥对隐写后的多媒体文件进行签名处理得到隐写后的多媒体文件的数字签名
S25
将经过签名处理的隐写后的多媒体文件拼接在作为数字资产的多媒体文件数据后
S26
扰乱拼接处的数据块
S27
发布拼接在作为数字资产的多媒体文件数据后且拼接处的数据块被扰乱的经过签名处理的隐写后的多媒体文件
S28
结束

图 3

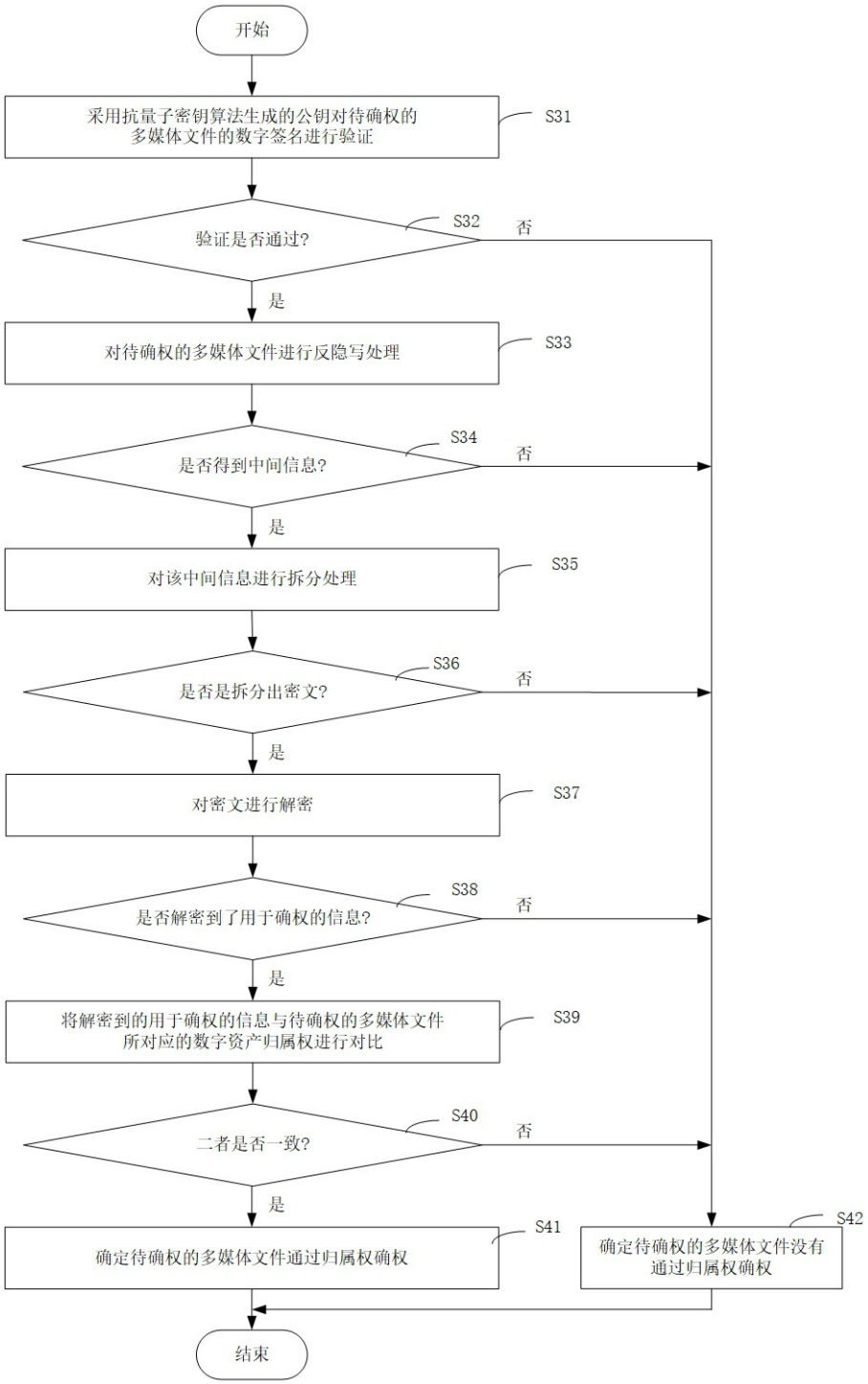

开始
采用抗量子密钥算法生成的公钥对待确权的多媒体文件的数字签名进行验证
S31
验证是否通过?
S32
否
是
对待确权的多媒体文件进行反隐写处理
S33
是否得到中间信息?
S34
否
是
对该中间信息进行拆分处理
S35
是否是拆分出密文?
S36
否
是
对密文进行解密
S37
是否解密到了用于确权的信息?
S38
否
是
将解密到的用于确权的信息与待确权的多媒体文件所对应的数字资产归属权进行对比
S39
二者是否一致?
S40
否
是
确定待确权的多媒体文件通过归属权确权
S41
确定待确权的多媒体文件没有通过归属权确权
S42
结束

图 4

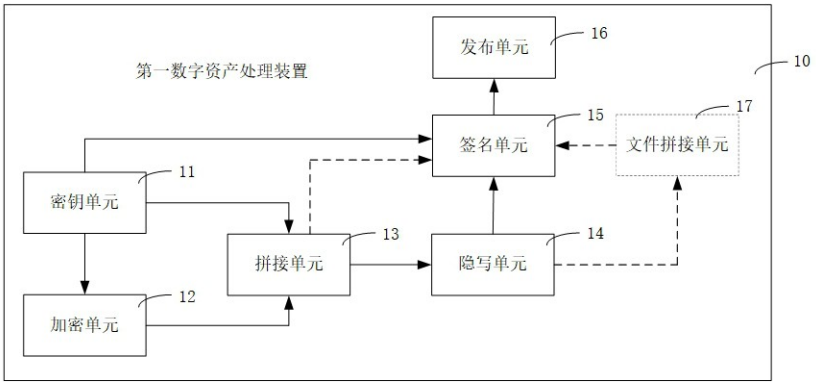

第一数字资产处理装置
发布单元
16
10
17
15
签名单元
文件拼接单元
11
密钥单元
13
14
拼接单元
隐写单元
12
加密单元

图 5

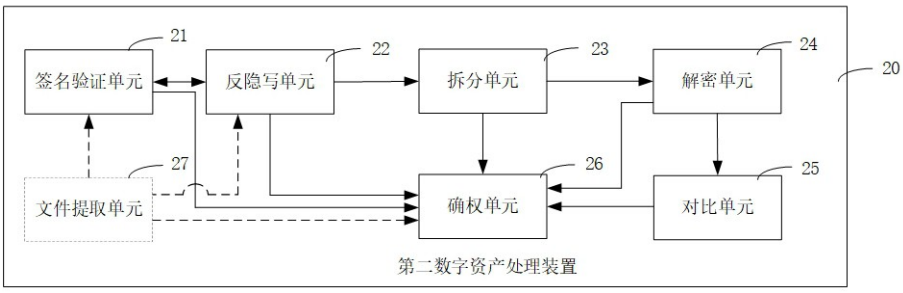

21
22
23
24
20
签名验证单元
反隐写单元
拆分单元
解密单元
27
26
25
文件提取单元
确权单元
对比单元
第二数字资产处理装置

图 6

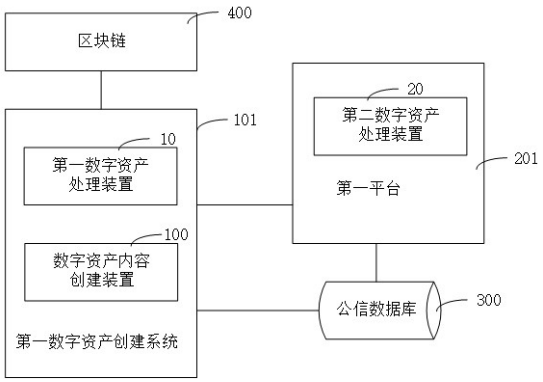

400
区块链
20
第二数字资产
处理装置
101
10
第一数字资产
处理装置
201
第一平台
100
数字资产内容
创建装置
公信数据库
300
第一数字资产创建系统

图 7

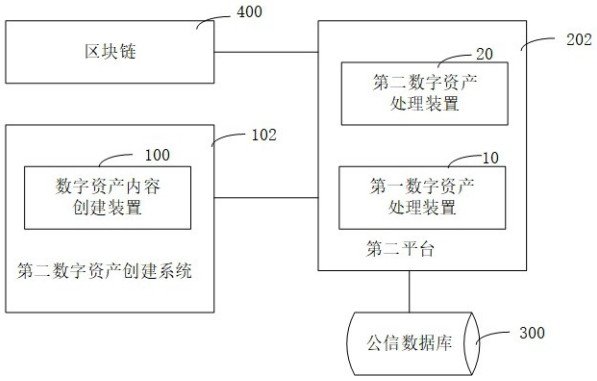

400
区块链
202
20
第二数字资产
处理装置
102
100
数字资产内容
创建装置
10
第一数字资产
处理装置
第二数字资产创建系统
第二平台
公信数据库
300

图 8

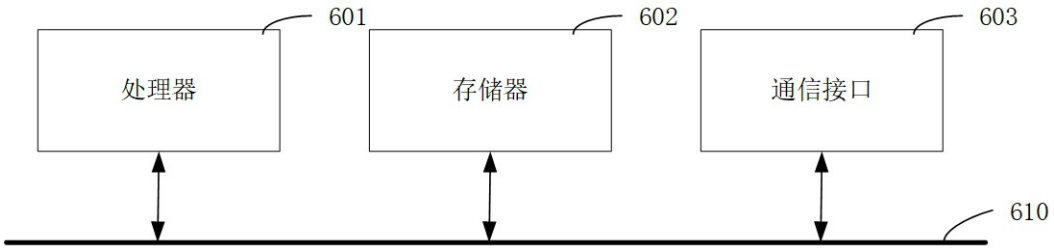

601
处理器
602
存储器
603
通信接口
610

图 9