

元数据的生成方法、验证方法及电子设备

5 技术领域

本申请实施例涉及数据处理领域，尤其涉及一种元数据的生成方法、验证方法及电子设备。

背景技术

随着人工智能（Artificial Intelligence，AI）技术的发展，AI 产生内容（Artificial Intelligence Generated Content，AIGC）成井喷式发展；AI 可以生成（或基于原有媒体内容进行修改）得到新颖、有趣、多样的数字内容（如图像、音乐和自然语言），以满足不同用户的喜好和场景。

然而，对媒体内容的修改加剧了一些错误信息和虚假信息的传播，使得用户无法判断媒体内容的真实性；因此，如何帮助用户判断媒体内容真实性十分重要。

15 发明内容

为了解决用户无法判断媒体内容真实性的问题，本申请提供一种元数据的生成方法、验证方法及电子设备；该生成方法生成的元数据可以用于媒体内容的溯源，能够一定程度帮助用户判断媒体内容的真实性。

一方面，本申请实施例提供一种元数据的生成方法，所述方法包括：

获取第一媒体内容；

20 生成所述第一媒体内容的元数据，所述第一媒体内容的元数据包括：所述第一媒体内容的初始信息、第一媒体哈希值和第一数字签名；所述第一媒体哈希值是所述第一媒体内容的哈希值，所述第一数字签名是第一数据的数字签名，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据。

示例性地，该方法包括：首先，获取第一媒体内容；接着，生成第一媒体内容的元数据，第一媒体内容的元数据包括：第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名；第一媒体哈希值是所述第一媒体内容的哈希值，第一组合哈希值是根据初始信息和第一媒体哈希值确定的。

其中，第一媒体哈希值可以用于验证元数据是不是第一媒体内容的元数据；初始信息可以用于第一媒体内容的初始身份证明，可以作为第一媒体内容真实性的一个维度的证明；第一数字签名可以用于验证初始信息和第一媒体哈希值是否被篡改。这样，元数据可以用于第一媒体内容的溯源；进而，可以一定程度帮助用户判断媒体内容的真实性。

30 示例性地，第一媒体内容的初始信息可以是指第一媒体内容生成时产生的信息。示例性地，第一媒体内容的初始信息可以包括多种信息。需要说明的是，初始信息所包含的信息种类可以根据场景以及媒体类型等确定，不同场景以及不同媒体类型对应的初始信息所包含的信息种类可以不同，本申请对此不作限制。也就是说，可以根据场景以及媒体类型，预先约定初始信息包含的信息种类；这样，能够增加元数据的可读性。

示例性地，所述第一数据是至少由所述第一媒体哈希值和所述第一媒体内容的初始信息组合后的数据，或者，所述第一数据是至少由所述初始信息的哈希值和所述第一媒体哈希值的哈希值组合后的数据。

示例性地，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的哈希值。

40 示例性地，所述第一数据是至少由所述第一媒体哈希值的哈希值和所述第一媒体内容的初始信息的哈希值确定的哈希值，或者，所述第一数据是至少由所述初始信息和所述第一媒体哈希值组合后的数据的哈希值。

示例性地，所述第一媒体内容的元数据还包括所述第一数据。

示例性地，所述第一媒体内容的元数据还包括所述第一媒体哈希值的哈希值和所述第一媒体内容的初始信息的哈希值。

45 示例性地，所述第一媒体内容的元数据还包括：第一统一资源定位符（URL），所述第一 URL 指示所述第一媒体内容的初始信息或所述第一媒体哈希值在所述第一媒体内容的元数据中的位置。

示例性地，所述第一数据是至少由所述第一媒体哈希值的哈希值、所述第一媒体内容的初始信息的哈希值和所述第一统一资源定位符组合后的数据的哈希值。

示例性地，所述生成所述第一媒体内容的元数据包括：  
获取所述第一媒体内容的初始信息和所述第一媒体哈希值；  
至少封装所述第一媒体内容的初始信息、所述第一媒体哈希值，得到第一封装数据（Trust Indicators）；  
对所述第一媒体哈希值进行哈希计算，得到所述第一媒体哈希值的哈希值；对所述第一媒体内容的初  
5 始信息进行哈希计算，得到所述第一媒体内容的初始信息的哈希值；  
至少封装所述第一媒体哈希值的哈希值和所述第一媒体内容的初始信息的哈希值，得到第二封装数据  
（Declaration Hash）；  
对所述第一数据进行数字签名，所述第一数据是至少由所述第一媒体哈希值的哈希值和所述第一媒体  
内容的初始信息的哈希值确定的数据，得到所述第一数字签名；  
10 至少封装所述第一封装数据、所述第二封装数据和所述第一数字签名，得到信任声明；  
至少根据所述信任声明得到所述第一媒体内容的元数据。  
示例性地，所述生成所述第一媒体内容的元数据包括：  
获取所述第一媒体内容的初始信息和所述第一媒体哈希值；  
至少封装所述第一媒体内容的初始信息、所述第一媒体哈希值，得到第一封装数据（Trust Indicators）；  
15 对所述第一数据进行数字签名，得到所述第一数字签名，所述第一数据是至少由所述第一媒体哈希值  
和所述第一媒体内容的初始信息确定的数据；  
至少封装所述信任指标和所述第一组合哈希值的数字签名，得到信任声明；  
至少根据所述信任声明得到所述第一媒体内容的元数据。  
示例性地，元数据可以包括用于描述媒体内容的数据；例如，元数据可以包括描述媒体内容属性  
20 （property）的信息。其中，元数据可以为信任档案（Trust Profile，信任档案也可以称为信任清单（Trust  
Manifest））。其中，Trust Profile 可以用于记录媒体内容生成以及变迁的相关信息，可以用于媒体内容的  
溯源。  
示例性地，第一媒体内容可以是指没有 Trust Profile 的媒体内容，其中，第一媒体内容包括但不限于：  
图像、图形、音频以及视频。  
25 示例性地，第一媒体内容可以是第一电子设备生成的媒体内容，也可以是第一电子设备从其他电子设  
备接收到的媒体内容。例如，第一媒体内容为图像，则第一媒体内容可以是第一电子设备拍摄的图像或截  
图或 AI 生成的图像等，本申请对第一电子设备生成图像的方式不作限制；第一媒体内容也可以是第一电  
子设备从其他电子设备接收到的图像，本申请对此不作限制。  
示例性地，可以采用哈希算法对第一媒体内容进行哈希计算，得到第一媒体哈希值；其中，本申请对  
30 计算第一媒体哈希值所采用的哈希算法不作限制。  
示例性地，可以采用哈希算法对第一媒体内容和初始信息的组合进行哈希计算，得到第一组合哈希值；  
也就是说，第一组合哈希值是第一媒体内容和初始信息组合的哈希值。其中，本申请对计算第一组合哈希  
值所采用的哈希算法不作限制。示例性地，当初始信息包括多种信息时，可以先将各种初始信息组合后再  
与第一媒体哈希值组合。  
35 示例性地，可以采用第一私钥对第一组合哈希值进行数字签名，得到第一组合哈希值的数字签名。具  
体地，可以基于数字签名算法，采用第一私钥对第一组合哈希值进行数字签名，得到第一组合哈希值的数  
字签名。应该理解的是，本申请对计算第一组合哈希值的数字签名所涉及的数字签名算法不作限制。其中，  
第一方面的方法可以应用于第一电子设备中，第一私钥可以是第一电子设备的私钥，即第一私钥与第一电  
子设备对应。另一种方式中，第一私钥可以是与第一电子设备对应的第一用户的私钥，即第一私钥与第一  
40 用户对应。  
第二方面，本申请实施例提供一种元数据的生成方法，所述方法包括：获取第 N+1 媒体内容，所述第  
N+1 媒体内容基于第 N 媒体内容得到；生成所述第 N+1 媒体内容的元数据，所述第 N+1 媒体内容的元数  
据包括第一媒体内容的初始信息和第一数据的数字签名；所述 N+1 媒体内容的元数据还包括 N 个媒体哈  
希值，其中，第一媒体哈希值是所述第一媒体内容的哈希值，第 N+1 媒体哈希值是所述第 N+1 媒体内容  
45 的哈希值，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据；N 为正整数。  
示例性地，一种元数据的生成方法，该方法包括：首先，获取第 N+1 媒体内容，第 N+1 媒体内容基  
于第 N 媒体内容得到；生成第 N+1 媒体内容的元数据，第 N+1 媒体内容的元数据包括第一媒体内容的初  
始信息、第一组合哈希值和第一组合哈希值的数字签名；N+1 媒体内容的元数据还包括 N+1 个媒体哈希

值, 其中, 第  $N+1$  媒体哈希值是第  $N+1$  媒体内容的哈希值, 第一组合哈希值是根据初始信息和第一媒体哈希值确定的, 第一媒体哈希值是第一媒体内容的哈希值;  $N$  为正整数。

其中, 第  $N+1$  媒体内容可以包括: 对第  $N$  媒体内容进行编辑处理之后得到的媒体内容, 或者, 对第  $N$  媒体内容的元数据进行修改所得到的媒体内容, 或者, 待转发(或分享)的第  $N$  媒体内容。应该理解的是, 第  $N$  并不构成对具体数量的限制, 只是为了便于区分。

也就是说, 在对第  $N$  媒体内容进行编辑处理之后, 或者在对第  $N$  媒体内容的元数据进行修改之后, 或者, 转发在第  $N$  媒体内容的过程中, 可以在第  $N$  媒体内容的元数据的基础上, 生成第  $N+1$  媒体内容的元数据; 这样, 可以将媒体内容的变迁过程记录在元数据, 进而保证通过对媒体内容的元数据的验证, 实现对媒体内容的溯源。

示例性地, 第  $N+1$  媒体哈希值是第  $N+1$  媒体内容的哈希值, 以此类推, 第  $N$  媒体哈希值是第  $N$  媒体内容的哈希值, 第  $N-1$  媒体哈希值是第  $N-1$  媒体内容的哈希值.....

示例性地, 可以采用哈希算法对第  $N+1$  媒体内容进行哈希计算, 得到第  $N+1$  媒体哈希值; 其中, 本申请对计算第  $N+1$  媒体哈希值所采用的哈希算法不作限制。

根据第二方面, 第  $N+1$  媒体内容的元数据还包括  $N$  个组合哈希值和  $N$  个组合哈希值的数字签名; 其中, 第  $N+1$  组合哈希值是根据第  $N$  组合哈希值和第  $N+1$  媒体哈希值确定的。这样, 可以将第  $N$  组合哈希值和第  $N+1$  媒体哈希值进行关联, 以防止元数据中的部分信息被伪造。

根据第二方面, 第  $N+1$  媒体内容的元数据还包括  $N$  个组合哈希值和  $N$  个组合哈希值的数字签名; 其中, 第  $N+1$  组合哈希值是根据第  $N$  组合哈希值、第  $N$  组合哈希值的数字签名和第  $N+1$  媒体哈希值确定的。这样, 可以防止元数据中的部分信息被伪造。

根据第二方面, 或者以上第二方面的任意一种实现方式, 第  $N+1$  媒体内容的元数据还包括一个或多个第  $N+1$  媒体声明和一个或多个第  $N+1$  声明哈希值; 其中, 第  $N+1$  媒体声明为对第  $N+1$  媒体内容的声明, 第  $N+1$  声明哈希值为第  $N+1$  媒体声明的哈希值。

示例性地, 声明可以包括但不限于: 版权信息, 缩略图、是否可以被修改, 操作权限、使用权限、第  $N+1$  媒体内容的来源、编辑信息等等。

应该理解的是, 第  $N+1$  媒体声明和第  $N+1$  声明哈希值为可选信息, 也就是说, 可以在生成元数据的过程中, 针对第  $N+1$  媒体内容进行声明, 也可以不对第  $N+1$  媒体内容进行声明; 这样, 可以提高元数据的灵活性和向后兼容能力。

根据第二方面, 或者以上第二方面的任意一种实现方式, 第  $N+1$  组合哈希值进一步根据一个或多个第  $N+1$  声明哈希值确定的。也就是说, 第  $N+1$  组合哈希值可以是根据第  $N$  组合哈希值、第  $N+1$  媒体哈希值和一个或多个第  $N+1$  声明哈希值确定的。这样, 可以将第  $N$  组合哈希值、第  $N+1$  媒体哈希值和一个或多个第  $N+1$  声明哈希值关联, 以防止元数据中的部分信息被伪造。

根据第二方面, 或者以上第二方面的任意一种实现方式, 将第  $N$  组合哈希值、一个或多个第  $N+1$  声明哈希值和第  $N+1$  媒体哈希值中的一个或多个哈希值连接后进行哈希计算, 得到中间哈希值; 其中, 中间哈希值用于确定第  $N+1$  组合哈希值。

当中间哈希值是采用第  $N$  组合哈希值、一个或多个第  $N+1$  声明哈希值和第  $N+1$  媒体哈希值中所有哈希值连接后进行哈希计算得到的, 则可以将中间哈希值作为第  $N+1$  组合哈希值。

当中间哈希值是采用第  $N$  组合哈希值、一个或多个第  $N+1$  声明哈希值和第  $N+1$  媒体哈希值中部分哈希值连接后进行哈希计算得到的, 则可以根据中间哈希值与第  $N$  组合哈希值、一个或多个第  $N+1$  声明哈希值和第  $N+1$  媒体哈希值中另一部分哈希值进行哈希计算, 得到第  $N+1$  组合哈希值。

根据第二方面, 或者以上第二方面的任意一种实现方式, 将第  $N$  组合哈希值、第  $N$  组合哈希值的数字签名、一个或多个第  $N+1$  声明哈希值和第  $N+1$  媒体哈希值中的一个或多个哈希值连接后进行哈希计算, 得到中间哈希值; 其中, 中间哈希值用于确定第  $N+1$  组合哈希值。

当中间哈希值是采用第  $N$  组合哈希值、第  $N$  组合哈希值的数字签名、一个或多个第  $N+1$  声明哈希值和第  $N+1$  媒体哈希值中所有哈希值连接后进行哈希计算得到的, 则可以将中间哈希值作为第  $N+1$  组合哈希值。

当中间哈希值是采用第  $N$  组合哈希值、第  $N$  组合哈希值的数字签名、一个或多个第  $N+1$  声明哈希值和第  $N+1$  媒体哈希值中部分哈希值连接后进行哈希计算得到的, 则可以根据中间哈希值与第  $N$  组合哈希值、一个或多个第  $N+1$  声明哈希值和第  $N+1$  媒体哈希值中另一部分哈希值进行哈希计算, 得到第  $N+1$  组

合哈希值。

应该理解的是，本申请对计算第 N+1 组合哈希值所采用的哈希算法不作限制。

根据第二方面，或者以上第二方面的任意一种实现方式，第 N+1 组合哈希值是采用哈希树，对第 N 组合哈希值、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值进行哈希计算得到的；哈希树包括根节点和叶子节点；第 N+1 组合哈希值是哈希树的根节点的值，第 N 组合哈希值、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值分别为哈希树的叶子节点的值。

根据第二方面，或者以上第二方面的任意一种实现方式，第 N+1 组合哈希值是采用哈希树，对第 N 组合哈希值、第 N 组合哈希值的数字签名、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值进行哈希计算得到的；哈希树包括根节点和叶子节点；第 N+1 组合哈希值是哈希树的根节点的值，第 N 组合哈希值、第 N 组合哈希值的数字签名、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值分别为哈希树的叶子节点的值。

示例性地，哈希树是一种数据结构。

根据第二方面，或者以上第二方面的任意一种实现方式，第 N+1 组合哈希值是采用哈希树，对第 N 组合哈希值、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值进行哈希计算得到的；哈希树包括左子树和右子树；第 N+1 组合哈希值是哈希树的根节点的值，第 N 组合哈希值为左子树的根节点的值，第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值分别为右子树的叶子节点的值。

根据第二方面，或者以上第二方面的任意一种实现方式，第 N+1 组合哈希值是采用哈希树，对第 N 组合哈希值、第 N 组合哈希值的数字签名、第 N+1 媒体哈希值和所述一个或多个第 N+1 声明哈希值进行哈希计算得到的；哈希树包括左子树和右子树；第 N+1 组合哈希值是所述哈希树的根节点的值，第 N 组合哈希值和第 N 组合哈希值的数字签名分别为左子树的根节点的子节点的值，第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值分别为右子树的叶子节点的值。

根据第二方面，或者以上第二方面的任意一种实现方式，哈希树为默克尔树 Merkle Tree。这样，当元数据数据量较大时，可以对 Merkle Tree 进行剪枝，以降低元数据占用的内存。

应该理解的是，哈希树还可以包括但不限于二叉树、三叉树等等，本申请对此不作限制。

根据第二方面，或者以上第二方面的任意一种实现方式，第 N+1 组合哈希值的数字签名是采用第 N+1 私钥对第 N+1 组合哈希值进行数字签名得到的。

示例性地，可以采用第 N+1 私钥对第 N+1 组合哈希值进行数字签名，得到第 N+1 组合哈希值的数字签名。具体地，可以基于数字签名算法，采用第 N+1 私钥对第 N+1 组合哈希值进行数字签名，得到第 N+1 组合哈希值的数字签名。应该理解的是，本申请对计算第 N+1 组合哈希值的数字签名所涉及的数字签名算法不作限制。其中，第二方面以及第二方面的任意一种实现方式可以应用于第 N+1 电子设备中，第 N+1 私钥可以是第 N+1 电子设备的私钥，即第 N+1 私钥与第 N+1 电子设备对应。另一种方式中，第 N+1 私钥可以是与第 N+1 电子设备对应的第 N+1 用户的私钥，即第 N+1 私钥与第 N+1 用户对应。

当然，第二方面以及第二方面的任意一种实现方式可以应用于第一电子设备中，第 N+1 私钥可以是第一电子设备的私钥，即第 N+1 私钥与第一电子设备对应。另一种方式中，第 N+1 私钥可以是与第一电子设备对应的第一用户的私钥，即第 N+1 私钥与第一用户对应。

需要说明的是，N+1 个私钥中的任意两个私钥可以相同也可以不同，具体可以根据生成元数据的用户和电子设备确定，本申请对此不作限制。

根据第二方面，或者以上第二方面的任意一种实现方式，该方法还包括：根据初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名，得到信任声明（Trust Declaration）。这样，便于元数据的管理与存储；也能够提高后续验证过程中的验证效率。

示例性地，可以将初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名封装，以得到 Trust Declaration。

根据第二方面，或者以上第二方面的任意一种实现方式，根据第 N+1 媒体哈希值、第 N+1 组合哈希值和第 N+1 组合哈希值的数字签名，得到信任记录（Trust Record）。这样，便于元数据的管理与存储；也能够提高后续验证过程中的验证效率。

示例性地，将第 N+1 媒体哈希值、第 N+1 组合哈希值和第 N+1 组合哈希值的数字签名封装，以得到 Trust Record。

根据第二方面，或者以上第二方面的任意一种实现方式，该方法还包括：根据信任声明和信任记录，

得到第 N+1 媒体内容的信任档案 (Trust Profile)。

示例性地, 可以将信任声明和信任记录封装以得到第 N+1 媒体内容 Trust Profile。

根据第二方面, 或者以上第二方面的任意一种实现方式, 第一媒体内容的初始信息包括以下至少一种: 第一媒体内容的生成时间、第一媒体内容的作者名称、第一媒体内容的数字内容标识、第一媒体内容的生成地点、第一媒体内容的生成设备的信息、第一媒体内容的分辨率、第一媒体内容的大小、第一媒体内容的媒体类型或第一媒体内容的生成方式。

应该理解的是, 初始信息还可以包括其他信息, 本申请对此不作限制。

根据第二方面, 所述第 N+1 媒体内容的元数据还包括第 N+1 声明。

根据第二方面, 所述第 N+1 媒体内容的元数据还包括第 N+1 媒体哈希值的哈希值和第 N+1 声明的哈希值。

根据第二方面, 所述第 N+1 媒体内容的元数据还包括 N 个数字签名, 所述第 N+1 数字签名是第 N+1 数据的数字签名, 所述第 N+1 数据是基于至少根据所述 N+1 声明和所述第 N+1 媒体哈希值确定的数据。

根据第二方面, 所述第 N+1 数据是至少根据所述 N+1 声明和所述第 N+1 媒体哈希值确定的哈希值。

根据第二方面, 所述第 N+1 数据是至少由所述 N+1 声明的哈希值和所述第 N+1 媒体哈希值的哈希值确定的哈希值, 或者, 所述第 N+1 数据是至少由所述第 N+1 声明和所述第 N+1 媒体哈希值组合后的数据的哈希值。

根据第二方面, 所述第 N+1 媒体内容的元数据还包括: 第 N+1 统一资源定位符 (URL), 所述第 N+1 URL 指示所述第 N+1 声明和所述第 N+1 媒体哈希值在所述第 N+1 媒体内容的元数据中的位置。

根据第二方面, 所述第 N+1 数据是至少由所述第 N+1 声明的哈希值、所述第 N+1 媒体哈希值的哈希值和所述第 N+1 URL 组合后的数据的哈希值。

第三方面, 本申请实施例提供了一种验证方法, 该方法包括: 首先, 获取第一媒体内容的元数据; 其中, 元数据包括: 第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名; 第一媒体哈希值是第一媒体内容的哈希值, 第一组合哈希值是根据初始信息和第一媒体哈希值确定的; 接着, 对第一媒体内容的元数据进行验证。

示例性地, 可以对第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名分别进行验证; 当对第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名中至少一个验证失败时, 可以确定第一媒体内容的元数据为假; 此时, 用户可以进一步对第一媒体内容的真实性进行判断, 或者, 确定第一媒体内容中的内容为假, 本申请对此不作限制。当对第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名的验证均成功时, 可以说明第一媒体内容的元数据为真。此时, 用户可以进一步对第一媒体内容的真实性进行判断, 或者, 确定第一媒体内容中的内容为真, 本申请对此不作限制。

第四方面, 本申请实施例提供了一种验证方法, 该方法包括: 首先, 获取第 N+1 媒体内容的元数据; 其中, 第 N+1 媒体内容的元数据包括第一媒体内容的初始信息、第一组合哈希值和第一组合哈希值的数字签名; N+1 媒体内容的元数据还包括 N+1 个媒体哈希值, 其中, 第 N+1 媒体哈希值是第 N+1 媒体内容的哈希值, 第一组合哈希值是根据初始信息和第一媒体哈希值确定的, 第一媒体哈希值是第一媒体内容的哈希值; N 为正整数; 接着, 对第 N+1 媒体内容的元数据进行验证。

示例性地, 可以对 N+1 个媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名分别进行验证; 当对 N+1 个媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名中至少一个验证失败时, 可以确定第 N+1 媒体内容的元数据为假; 此时, 用户可以进一步对第 N+1 媒体内容的真实性进行判断, 或者, 确定第 N+1 媒体内容中的内容为假, 本申请对此不作限制。当对 N+1 个媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名的验证均成功时, 可以说明第 N+1 媒体内容的元数据为真。此时, 用户可以进一步对第 N+1 媒体内容的真实性进行判断, 或者, 确定第 N+1 媒体内容中的内容为真, 本申请对此不作限制。

第五方面, 本申请实施例提供了一种元数据的生成装置, 该装置包括:

第一数据获取模块, 用于获取第一媒体内容;

第一信息生成模块, 用于生成第一媒体内容的元数据, 第一媒体内容的元数据包括: 第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名; 第一媒体哈希值是第一媒体内容的哈希值, 第一组合哈希值是初始信息和第一媒体哈希值的组合的哈希值。

示例性地, 元数据的生成装置还可以包括:

第一哈希计算模块, 用于对第一媒体内容进行哈希计算, 得到第一媒体哈希值。

示例性地, 第一哈希计算模块, 还用于根据初始信息和第一媒体哈希值的组合进行哈希计算, 得到第一组合哈希值。

示例性地, 元数据的生成装置还可以包括:

- 5 第一封装模块, 用于根据第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名, 得到信任声明。

第五方面以及第五方面的任意一种实现方式分别与第一方面以及第一方面的任意一种实现方式相对应。第五方面以及第五方面的任意一种实现方式所对应的技术效果可参见上述第一方面以及第一方面的任意一种实现方式所对应的技术效果, 此处不再赘述。

- 10 第六方面, 本申请实施例提供了一种元数据的生成装置, 该装置包括:

第二数据获取模块, 获取第 N+1 媒体内容, 第 N+1 媒体内容基于第 N 媒体内容得到;

第二信息生成模块, 用于生成第 N+1 媒体内容的元数据, 第 N+1 媒体内容的元数据包括第一媒体内容的初始信息、第一组合哈希值和第一组合哈希值的数字签名, 第一组合哈希值是初始信息和第一媒体哈希值的组合的哈希值; N+1 媒体内容的元数据还包括 N+1 个媒体哈希值, 其中, 第 N+1 媒体哈希值是第 N+1 媒体内容的哈希值, 第一媒体哈希值是第一媒体内容的哈希值; N 为正整数。

- 15 示例性地, 元数据的生成装置还可以包括:

第二哈希计算模块, 用于将第 N 组合哈希值、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中的一个或多个哈希值连接后进行哈希计算, 得到中间哈希值; 其中, 中间哈希值用于确定第 N+1 组合哈希值。

- 20 示例性地, 第二哈希计算模块, 还用于基于中间哈希值, 确定第 N+1 组合哈希值。

示例性地, 第二哈希计算模块, 还用于对第 N+1 媒体内容进行哈希计算, 得到第 N+1 媒体哈希值。

示例性地, 元数据的生成装置还可以包括:

第二封装模块, 用于根据初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名, 得到信任声明。

- 25 示例性地, 第二封装模块, 还用于根据第 N+1 媒体哈希值、第 N+1 组合哈希值和第 N+1 组合哈希值的数字签名, 得到信任记录。

示例性地, 第二封装模块, 还用于根据信任声明和信任记录, 得到第 N+1 媒体内容的信任档案。

应该理解的是, 第六方面的元数据的生成装置可以执行第二方面以及第二方面的任意一种实现方式中的步骤, 在此不再赘述。

- 30 第六方面以及第六方面的任意一种实现方式分别与第二方面以及第二方面的任意一种实现方式相对应。第六方面以及第六方面的任意一种实现方式所对应的技术效果可参见上述第二方面以及第二方面的任意一种实现方式所对应的技术效果, 此处不再赘述。

需要说明的是, 当第五方面的元数据的生成装置与第六方面的元数据的生成装置属于同一电子设备时, 则第五方面的元数据的生成装置与第六方面的元数据的生成装置为同一装置; 此时, 第一数据获取模块与第二数据获取模块为同一模块, 第一信息生成模块和第二信息生成模块为同一模块, 第一哈希计算模块和第二哈希计算模块为同一模块, 以及第一封装模块和第二封装模块为同一模块。

- 35 当第五方面的元数据的生成装置与第六方面的元数据的生成装置属于不同的电子设备时, 则第五方面的元数据的生成装置与第六方面的元数据的生成装置为不同的两个装置; 此时, 第一数据获取模块与第二数据获取模块是不同的两个模块, 第一信息生成模块和第二信息生成模块是不同的两个模块, 第一哈希计算模块和第二哈希计算模块是不同的两个模块, 以及第一封装模块和第二封装模块是不同的两个模块。

- 40 第七方面, 本申请实施例提供了一种验证装置, 该装置包括:

第一信息获取模块, 用于获取第一媒体内容的元数据; 其中, 元数据包括: 第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名; 第一媒体哈希值是第一媒体内容的哈希值, 第一组合哈希值是初始信息和第一媒体哈希值的组合的哈希值;

- 45 第一验证模块, 用于对第一媒体内容的元数据进行验证。

第八方面, 本申请实施例提供了一种元验证装置, 该装置包括:

第二信息获取模块, 用于获取第 N+1 媒体内容的元数据; 其中, 第 N+1 媒体内容基于第 N 媒体内容得到, 第 N+1 媒体内容的元数据包括第一媒体内容的初始信息、第一组合哈希值和第一组合哈希值的数字

签名, 第一组合哈希值是初始信息和第一媒体哈希值的组合的哈希值; N+1 媒体内容的元数据还包括 N+1 个媒体哈希值, 其中, 第 N+1 媒体哈希值是第 N+1 媒体内容的哈希值, 第一媒体哈希值是第一媒体内容的哈希值; N 为正整数;

第二验证模块, 用于对第 N+1 媒体内容的元数据进行验证。

- 5 需要说明的是, 当第七方面的验证装置与第八方面的验证装置属于同一电子设备时, 则第七方面的验证装置与第八方面的验证装置为同一装置; 此时, 第一信息获取模块与第二信息获取模块为同一模块, 以及第一验证模块和第二验证模块为同一模块。当第七方面的验证装置与第八方面的验证装置属于不同的两个电子设备时, 则第七方面的验证装置与第八方面的验证装置为不同的两个装置; 此时, 第一信息获取模块与第二信息获取模块是不同的两个模块, 以及第一验证模块和第二验证模块是不同的两个模块。

- 10 第九方面, 本申请实施例提供一种电子设备, 包括: 存储器和处理器, 存储器与处理器耦合; 存储器存储有程序指令, 当程序指令由处理器执行时, 使得电子设备执行第一方面或第一方面的任意可能的实现方式中的元数据的生成方法。

- 第九方面以及第九方面的任意一种实现方式分别与第一方面以及第一方面的任意一种实现方式相对应。第九方面以及第九方面的任意一种实现方式所对应的技术效果可参见上述第一方面以及第一方面的任意一种实现方式所对应的技术效果, 此处不再赘述。

- 15 第十方面, 本申请实施例提供一种电子设备, 包括: 存储器和处理器, 存储器与处理器耦合; 存储器存储有程序指令, 当程序指令由处理器执行时, 使得电子设备执行第二方面或第二方面的任意可能的实现方式中的元数据的生成方法。

- 第十方面以及第十方面的任意一种实现方式分别与第二方面以及第二方面的任意一种实现方式相对应。第十方面以及第十方面的任意一种实现方式所对应的技术效果可参见上述第二方面以及第二方面的任意一种实现方式所对应的技术效果, 此处不再赘述。

- 第十一方面, 本申请实施例提供一种电子设备, 包括: 存储器和处理器, 存储器与处理器耦合; 存储器存储有程序指令, 当程序指令由处理器执行时, 使得电子设备执行第三方面或第三方面的任意可能的实现方式中的验证方法。

- 25 第十一方面以及第十一方面的任意一种实现方式分别与第三方面以及第三方面的任意一种实现方式相对应。第十一方面以及第十一方面的任意一种实现方式所对应的技术效果可参见上述第三方面以及第三方面的任意一种实现方式所对应的技术效果, 此处不再赘述。

- 第十二方面, 本申请实施例提供一种电子设备, 包括: 存储器和处理器, 存储器与处理器耦合; 存储器存储有程序指令, 当程序指令由处理器执行时, 使得电子设备执行第四方面或第四方面的任意可能的实现方式中的验证方法。

- 30 第十二方面以及第十二方面的任意一种实现方式分别与第四方面以及第四方面的任意一种实现方式相对应。第十二方面以及第十二方面的任意一种实现方式所对应的技术效果可参见上述第四方面以及第四方面的任意一种实现方式所对应的技术效果, 此处不再赘述。

- 35 第十三方面, 本申请实施例提供一种芯片, 包括一个或多个接口电路和一个或多个处理器; 一个或多个处理器通过一个或多个接口电路接收或发送数据, 当一个或多个处理器执行计算机指令时, 使得电子设备执行第一方面或第一方面的任意可能的实现方式中的元数据的生成方法, 或者, 使得电子设备执行第二方面或第二方面的任意可能的实现方式中的元数据的生成方法, 或者, 使得电子设备执行第三方面或第三方面的任意可能的实现方式中的验证方法; 或者, 使得电子设备执行第四方面或第四方面的任意可能的实现方式中的验证方法。

- 40 第十三方面以及第十三方面的任意一种实现方式分别与第一方面以及第一方面的任意一种实现方式相对应, 或者, 与第二方面以及第二方面的任意一种实现方式相对应, 或者, 与第三方面以及第三方面的任意一种实现方式相对应, 或者, 与第四方面以及第四方面的任意一种实现方式相对应。第十三方面以及第十三方面的任意一种实现方式所对应的技术效果可参见上述第一方面以及第一方面的任意一种实现方式所对应的技术效果, 或者, 参照第二方面以及第二方面的任意一种实现方式所对应的技术效果, 或者, 参照第三方面以及第三方面的任意一种实现方式所对应的技术效果, 或者, 参照第四方面以及第四方面的任意一种实现方式所对应的技术效果, 此处不再赘述。

- 45 第十四方面, 本申请实施例提供一种计算机可读存储介质, 计算机可读存储介质存储有计算机程序, 当计算机程序运行在计算机或处理器上时, 使得电子设备执行第一方面或第一方面的任意可能的实现方式

中的元数据的生成方法，或者，使得电子设备执行第二方面或第二方面的任意可能的实现方式中的元数据的生成方法，或者，使得电子设备执行第三方面或第三方面的任意可能的实现方式中的验证方法；或者，使得电子设备执行第四方面或第四方面的任意可能的实现方式中的验证方法。

第十四方面以及第十四方面的任意一种实现方式分别与第一方面以及第一方面的任意一种实现方式相对应，或者，与第二方面以及第二方面的任意一种实现方式相对应，或者，与第三方面以及第三方面的任意一种实现方式相对应，或者，与第四方面以及第四方面的任意一种实现方式相对应。第十四方面以及第十四方面的任意一种实现方式所对应的技术效果可参见上述第一方面以及第一方面的任意一种实现方式所对应的技术效果，或者，参照第二方面以及第二方面的任意一种实现方式所对应的技术效果，或者，参照第三方面以及第三方面的任意一种实现方式所对应的技术效果，或者，参照第四方面以及第四方面的任意一种实现方式所对应的技术效果，此处不再赘述。

第十五方面，本申请实施例提供一种计算机程序产品，计算机程序产品包括计算机指令，当计算机指令被计算机或处理器执行时，使得计算机或处理器执行第一方面或第一方面的任意可能的实现方式中的元数据的生成方法，或者，使得计算机或处理器执行第二方面或第二方面的任意可能的实现方式中的元数据的生成方法，或者，使得计算机或处理器执行第三方面或第三方面的任意可能的实现方式中的验证方法；或者，使得计算机或处理器执行第四方面或第四方面的任意可能的实现方式中的验证方法。

第十五方面以及第十五方面的任意一种实现方式分别与第一方面以及第一方面的任意一种实现方式相对应，或者，与第二方面以及第二方面的任意一种实现方式相对应，或者，与第三方面以及第三方面的任意一种实现方式相对应，或者，与第四方面以及第四方面的任意一种实现方式相对应。第十五方面以及第十五方面的任意一种实现方式所对应的技术效果可参见上述第一方面以及第一方面的任意一种实现方式所对应的技术效果，或者，参照第二方面以及第二方面的任意一种实现方式所对应的技术效果，或者，参照第三方面以及第三方面的任意一种实现方式所对应的技术效果，或者，参照第四方面以及第四方面的任意一种实现方式所对应的技术效果，此处不再赘述。

#### 附图说明

- 图 1 为示例性示出的应用场景示意图；  
图 2a 为示例性示出的元数据的生成过程示意图；  
图 2b 为示例性示出的 Trust Profile 示意图；  
图 2c 为示例性示出的元数据的生成过程示意图；  
图 3a 为示例性示出的 Trust Profile 的生成过程示意图；  
图 3b 为示例性示出的 Trust Profile 示意图；  
图 3c 为示例性示出的 Trust Profile 示意图；  
图 3d 为示例性示出的 Trust Profile 的生成过程示意图；  
图 3e 为示例性示出的 Trust Profile 示意图；  
图 4a 为示例性示出的元数据的生成过程示意图；  
图 4b 为示例性示出的 Trust Profile 示意图；  
图 4c 为示例性示出的元数据的生成过程示意图；  
图 5a 为示例性示出了 Trust Profile 的生成过程示意图；  
图 5b 为示例性示出的 Trust Profile 示意图；  
图 5c 为示例性示出的 Trust Profile 示意图；  
图 6a 为示例性示出的 Trust Profile 生成过程示意图；  
图 6b 为示例性示出的 Trust Profile 生成过程示意图；  
图 6c 为示例性示出的第 N+1 组合哈希值生成过程示意图；  
图 6d 为示例性示出的第 N+1 组合哈希值生成过程示意图；  
图 6e 为示例性示出的第 N+1 组合哈希值生成过程示意图；  
图 6f 为示例性示出的第 N+1 组合哈希值生成过程示意图；  
图 6g 为示例性示出的第 N+1 组合哈希值生成过程示意图；  
图 6h 为示例性示出的第 N+1 组合哈希值生成过程示意图；  
图 6i 为示例性示出的 Trust Profile 示意图；

- 图 6j 为示例性示出的 Trust Profile 示意图；  
图 7a 为示例性示出的 Trust Profile 的生成过程示意图；  
图 7b 为示例性示出的 Trust Profile 的生成过程示意图；  
图 7c 为示例性示出的 Trust Profile 示意图；  
5 图 8a 为示例性示出的 Trust Profile 的生成过程示意图；  
图 8b 为示例性示出的 Trust Profile 的生成过程示意图；  
图 8c 为示例性示出的 Trust Profile 示意图；  
图 8d 为示例性示出的 Trust Profile 示意图；  
图 9a 为示例性示出的验证过程示意图；  
10 图 9b 为示例性示出的验证过程示意图；  
图 10a 为示例性示出的验证过程示意图；  
图 10b 为示例性示出的验证过程示意图；  
图 10c 为示例性示出的验证过程示意图；  
图 10d 为示例性示出的验证过程示意图；  
15 图 10e 为示例性示出的验证过程示意图；  
图 11 为示例性示出的元数据的生成装置示意图；  
图 12 为示例性示出的元数据的生成装置示意图；  
图 13 为示例性示出的验证装置示意图；  
图 14 为示例性示出的验证装置示意图；  
20 图 15 为示例性示出的装置的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。

本申请实施例的说明书和权利要求书中的术语“第 N”和“第 N+1”等是用于区别不同的对象，而不是用于描述对象的特定顺序；其中，N 可以是一、二、三、四……等正整数。例如，第一目标对象和第二目标对象等是用于区别不同的目标对象，而不是用于描述目标对象的特定顺序。

在本申请实施例中，“示例性的”、“示例性地”或者“例如”等词用于表示作例子、例证或说明。本申请实施例中被描述为“示例性的”、“示例性地”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用““示例性的”、示例性地”或者“例如”等词旨在以具体方式呈现相关概念。

在本申请实施例的描述中，除非另有说明，“多个”的含义是指两个或两个以上。例如，多个处理单元是指两个或两个以上的处理单元；多个系统是指两个或两个以上的系统。

为了便于理解，首先对本申请实施例中提到的部分专业术语进行介绍。

1、媒体资产（Media Asset）

媒体资产可以包括媒体内容（Media Content）和媒体内容的元数据（Metadata）。其中，媒体内容的元数据与媒体内容是绑定的，或者说媒体内容的元数据与媒体内容是关联的）。

通常所说的获取媒体内容，也就是说获取该媒体内容的媒体资产；对应的，也获取到了该媒体内容的元数据。例如，获取图像，可以获取到图像和图像的元数据。

需要说明的是，部分场景中，媒体资产也被称为媒体文件或数字资产（Media Asset）。媒体资产可以是图象、音频、视频或者文本。

2、媒体内容（Media Content）

媒体内容，也可以称为数字内容（Digital content）。媒体内容可以是媒体资产的一部分，表示媒体的实际内容，数字内容是以数字形式存在的文本、图象、声音等不同内容类型的内容，它可以存储在如光盘、硬盘等数字载体上，并通过网络等手段传播。数字内容是将图像、文字、影音等内容通过数字技术进行整

合应用的产品或服务的总体，是数字媒体技术与文化创意结合的产物。例如，媒体内容可以是图象的像素数据，以及理解或呈现内容所需的任何附加技术元数据（例如，颜色配置文件或编码参数）。

数字技术（Digital Technology），是一项与电子计算机相伴相生的科学技术，它是指借助一定的设备将各种信息，包括：图、文、声、像等，转化为电子计算机能识别的二进制数字“0”和“1”后进行运算、加工、存储、传送、传播、还原的技术。由于在运算、存储等环节中要借助计算机对信息进行编码、压缩、解码等，因此也称为数码技术、计算机数字技术等。数字技术也称数字控制技术。

3、元数据（Metadata）

元数据可以包括用于描述媒体内容的数据；例如，元数据可以包括描述媒体内容属性（property）的信息。其中，示例性地，元数据可以为信任档案（或称为信任清单（Trust Manifest））。示例性地，元数据可以是媒体内容的创作位置、创建者、注释或 IPR 信息。

4、信任档案（Trust Profile）

媒体内容的 Trust Profile 可以是媒体内容的一种元数据，Trust Profile 记录了媒体内容生成以及变迁的相关信息，可以用于媒体内容的溯源。

5、数字内容标识

数字内容标识可以是指数字对象标识符（Digital Objects unique Identifier, DOI）。数字对象标识符，是一组由数字、字母或其他符号组成的字符串，用于标识数字化的内容资源。它可以分配给任何使用网络的数字实体。DOI 作为一个数字化对象的标识符具有唯一性，一旦产生就不会改变，不随其所标识的数字化对象的版权所有者或存储地址等属性的变更而改变。在传统的实体出版物中，图书、期刊、磁带、光盘等出版物都会以 ISBN（International Standard Book Number, 国际标准书号）、ISSN（International Standard Serial Number, 国际标准期刊号）、ISRC（International Standard Recording Code, 国际标准录音录像资料代码）等国际标准标识，并以条形码的形式贴在实物封面上作为出版物的唯一标识。这些标识使出版物得到有效便捷的管理，便于各个环节的查找和利用。而网上的文档一旦变更了网址（URL（Uniform Resource Location, 统一资源定位符）），就消失得无影无踪，让人无从追索。如果给数字信息加上数字对象标识符（DOI），就如同出版物上贴了条形码一样，无论到哪里都有迹可寻。因此，数字对象标识符（DOI）也被称为数字资源“条形码”。

图 1 为示例性示出的应用场景示意图。

当用户需要对该媒体内容进行溯源，或者需要判断该媒体内容的真实性时（其中，通过对媒体内容的溯源，可以一定程度帮助判断媒体内容的真实性），可以打开终端设备中的媒体溯源平台客户端（如应用程序、小程序、网页等）进行查询。

示例性地，用户 A 的手机 A 接收到用户 B 的手机 B 发送的媒体内容后，若用户 A 需要使用该媒体内容（如转发）时，可以先对该媒体内容进行溯源。在确定媒体内容的真实性后，再确定是否使用该媒体内容。

应该理解的是，手机 A 也可以是其他运算能力较强的电子设备，如个人计算机、计算机工作站、平板电脑等等，本申请对此不作限制。

示例性地，当用户需要判断智能手表中媒体内容的真实性时，可以将智能手表中的媒体内容发送给手机，由手机对该媒体内容进行溯源，然后发送溯源结果给智能手表。

应该理解的是，智能手表也可以是其他运算能力较弱的电子设备如媒体消费设备、可穿戴设备、机顶盒、游戏机等，本申请对此不作限制。手机也可以是其他运算能力较强的电子设备，如个人计算机、计算机工作站、平板电脑等等，本申请对此不作限制。

参照图 1（1），媒体溯源平台的主界面 101 可以包括一个或多个控件，包括但不限于：输入框、溯源按钮等等，本申请对此不作限制。

示例性地，用户可以点击输入框，媒体溯源平台可以响应于用户的操作行为，展示文件选择界面。接着，用户在文件选择界面中选取对应的媒体内容后，可以点击主界面 101 中的溯源按钮；对应的，媒体溯源平台可以响应于用户的操作行为，获取媒体内容的 Trust Profile；然后对 Trust Profile 进行验证。

示例性地，媒体溯源平台在完成对 Trust Profile 验证后，可以显示验证结果以及显示 Trust Profile 中的部分信息。其中，验证结果包括溯源验证成功和溯源验证失败。

参照图 1（2），图 1（2）中显示的验证结果为溯源验证成功，显示的 Trust Profile 中的信息可以包括媒体内容的生成时间、媒体内容的生成地点、媒体内容的生成设备名称、是否由 AI 生成。

参照图 1 (3), 图 1 (3) 中显示的验证结果为溯源验证失败; 且当溯源验证失败时, 可以对 Trust Profile 中溯源验证失败的信息与溯源验证成功的信息进行区分显示。如图 1 (3) Trust Profile 中验证成功的信息可以包括媒体内容的生成时间、媒体内容的生成地点、媒体内容的生成设备名称、是否由 AI 生成, Trust Profile 中验证失败的信息可以为数字签名。

5 一种可能的方式中, 可以由媒体溯源平台的客户端执行识别媒体内容的真实性。例如, 当待识别的媒体内容的真实性为一个时, 媒体溯源平台的客户端可以在本地进行识别。

一种可能的方式中, 可以由媒体溯源平台的服务端识别媒体内容的真实性。例如, 当待识别的媒体内容为多个时, 媒体溯源平台的客户端可以将多个待识别的媒体内容发送给媒体溯源平台的服务端, 由媒体溯源平台的服务端识别媒体内容的真实性, 并将识别结果返回给媒体溯源平台的客户端。

10 需要说明的是, 本申请中是由媒体溯源平台的客户端识别媒体内容的真实性, 还是由媒体溯源平台的服务器识别媒体内容的真实性, 不受待识别的媒体内容的数量的限制。

以下对 Trust Profile 的生成过程和验证过程进行说明。

首先, 对 Trust Profile 的生成过程进行说明, 可以参照图 2a~图 8a 的实施例。

15 图 2a 为示例性示出的 Trust Profile 的生成过程示意图。其中, 由第一电子设备执行图 2a 的实施例中的步骤。

S201, 获取第一媒体内容。

示例性地, 第一媒体内容可以是指没有 Trust Profile 的媒体内容, 其中, 第一媒体内容可以是以数字形式存在的文本、图象、声音等不同内容类型的内容, 例如, 第一媒体内容可以是图象的像素数据, 以及理解或呈现内容所需的任何附加技术元数据 (例如, 颜色配置文件或编码参数)。

20 示例性地, 第一媒体内容可以是第一电子设备生成的媒体内容, 也可以是第一电子设备从其他电子设备接收到的媒体内容。例如, 第一媒体内容为图像, 则第一媒体内容可以是第一电子设备拍摄的图像或截图或 AI 生成的图像等, 本申请对第一电子设备生成图像的方式不作限制; 也可以是第一电子设备从其他电子设备接收到的图像, 本申请对此不作限制。

25 示例性地, 如图 2c 所示, S202, 生成第一媒体内容的元数据, 第一媒体内容的元数据包括: 第一媒体内容的初始信息、第一媒体哈希值和第一数字签名; 第一媒体哈希值是第一媒体内容的哈希值, 所述第一数字签名是第一数据的数字签名, 所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据。需要说明的是, 第一数据是第一媒体内容的元数据中可选记载的数据, 在第一媒体内容的元数据有第一数据的情况下, 可以方便验证哈希和签名; 在第一媒体内容的元数据没有第一数据的情况下, 可以节省空间。

30 示例性地, 第一数据是至少由第一媒体哈希值和第一媒体内容的初始信息组合后的数据, 或者, 第一数据是至少由初始信息的哈希值和第一媒体哈希值的哈希值组合后的数据。

示例性地, 第一数据也可作为第一组合哈希值, 第一组合哈希值包括第一媒体内容的初始信息和第一媒体哈希值组合后的哈希值。示例性地, 第一组合哈希值包括第一媒体内容的初始信息、第一媒体哈希值和其它描述性信息组合后的哈希值, 其它描述性信息可以不是初始信息中的其他描述性信息, 例如, 生成 Trust Profile 的工具的信息或者其它描述第一媒体内容的初始信息的信息, 本申请对此不作限制。

35 示例性地, 第一数据也可作为第一组合哈希值, 第一组合哈希值可以包括第一媒体内容的初始信息的哈希值和第一媒体哈希值的哈希值 (Media Hash 0.Hash) 组合后的哈希值。示例性地, 第一组合哈希值是第一媒体内容的初始信息的哈希值、第一媒体哈希值的哈希值和其它元数据信息的哈希值组合后的哈希值。这里, 在第一媒体内容的初始信息包括至少两个的情况下, 第一媒体内容的初始信息的哈希值可以包括第一媒体内容的初始信息中的每一个的哈希值, 或者, 第一媒体内容的初始信息的哈希值可以包括第一媒体内容的所有初始信息组合后的哈希值。

示例性地, 第一媒体内容的元数据还包括上述第一数据。

40 示例性地, 如图 2a 所示, S202, 生成第一媒体内容的元数据, 第一媒体内容的元数据包括: 第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名; 第一媒体哈希值是第一媒体内容的哈希值, 第一组合哈希值是根据初始信息和第一媒体哈希值生成的。示例性地, S202 生成的第一媒体内容的元数据, 可以是指第一媒体内容的 Trust Profile。

示例性地, 获取到第一媒体内容的同时可以获取到第一媒体内容的元数据; 此时获取的第一媒体内容的元数据可以包括第一媒体内容的初始信息, 但不包括第一媒体内容的 Trust Profile; 本申请可以执行 S202,

生成第一媒体内容的 Trust Profile, 将第一媒体内容的 Trust Profile, 作为第一媒体内容的一种元数据。

其中, 第一媒体内容的初始信息可以是指第一媒体内容生成时产生的信息。示例性地, 第一媒体内容的初始信息包括以下至少一种: 第一媒体内容的生成时间、第一媒体内容的作者名称、第一媒体内容的数字内容标识、第一媒体内容的生成地点、第一媒体内容的生成设备的信息、第一媒体内容的分辨率、第一媒体内容的大小、第一媒体内容的媒体类型或第一媒体内容的生成方式。例如, 第一媒体内容的生成设备的信息可以包括设备的型号、相机的参数等, 相机的参数可以包括相机拍摄图片时的焦距、感光度、曝光度等。应该理解的是, 第一媒体内容的初始信息还可以包括其它信息例如版权信息等用于描述第一媒体内容的信息, 本申请对此不作限制。

示例性地, 媒体类型可以包括但不限于: 图像类、视频类、音频类以及图形类等。生成方式可以包括: AI 生成方式和非 AI 生成方式等。一种可能的方式中, 初始信息中的生成方式可以采用 AIGC 标识替换: 例如, 当第一媒体内容是由 AI 生成时, AIGC 标识的值为 1; 当第一媒体内容不是由 AI 生成时, AIGC 标识的值为 0。第一媒体内容的作者名称可以是第一媒体内容的创作者的名称或者第一媒体内容的拍摄设备名称, 本申请对此不作限制。

示例性地, 当第一媒体内容是第一电子设备生成的媒体内容时, 第一媒体内容的初始信息可以由第一用户自定义输入, 也可以由第一电子设备自动生成(无需第一用户输入)。示例性地, 可以根据第一媒体内容, 生成第一媒体哈希值; 接着, 至少根据第一媒体哈希值和初始信息, 生成第一组合哈希值; 之后, 生成第一组合哈希值的数字签名; 然后, 采用初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名, 生成第一媒体内容的 Trust Profile。图 2b 为示例性示出的 Trust Profile 示意图。

示例性地, 如图 2b 所示, 第一媒体内容的元数据可以包括第一媒体内容的初始信息、第一媒体哈希值和第一组合哈希值的数字签名。第一媒体内容的初始信息可以包括 Content ID (即第一媒体内容的数字内容标识)、AIGC (即 AIGC 标识, 表示第一媒体内容的一种生成方式)、Creation Info (即 Creation Information, 可以包括生第一媒体内容的成时间、第一媒体内容的作者名称、第一媒体内容的生成地点等)。

在图 2b 中, 第一媒体内容的 Trust Profile 包括: Content ID (即第一媒体内容的数字内容标识)、AIGC (即 AIGC 标识)、Creation Info (即 Creation Information, 可以包括生第一媒体内容的成时间、第一媒体内容的作者名称、第一媒体内容的生成地点等)、Media Hash 0 (即第一媒体哈希值)、Hash (TD) (即第一组合哈希值) 和 Signaturesk0 (即第一组合哈希值的数字签名)。

应该理解的是, 图 2b 仅是本申请第一媒体内容的 Trust Profile 的一个示例性, 第一媒体内容的 Trust Profile 中各个信息的位置或排列顺序可以按照需求设置, 本申请对此不作限制。

需要说明的是, 第一媒体哈希值可以用于验证 Trust Profile 是不是第一媒体内容的 Trust Profile; 初始信息可以用于第一媒体内容的初始身份证明, 可以作为第一媒体内容真实性的一个维度的证明; 第一组合哈希值和第一组合哈希值的数字签名, 可以用于验证初始信息和第一媒体哈希值是否被篡改。这样, Trust Profile 可以用于第一媒体内容的溯源。

需要说明的是, 初始信息所包含的信息种类可以根据场景以及媒体类型等确定, 不同场景以及不同媒体类型对应的初始信息所包含的信息种类可以不同, 本申请对此不作限制。也就是说, 可以根据场景以及媒体类型, 预先约定初始信息包含的信息种类; 这样, 能够增加 Trust Profile 的可读性。

图 3c 为示例性示出的 Trust Profile 示意图。

示例性地, 如图 3c 所示, 第一媒体内容的元数据还可以包括第一媒体内容的初始信息的哈希值和第一媒体哈希值的哈希值。例如, 第一媒体内容的初始信息的哈希值可以包括: 第一媒体内容的媒体类型的哈希值 (Media Type. Hash)、第一媒体内容的生成方式的哈希值 (例如, AIGC 生成方式的哈希值 AIGC. Hash)。图 3a 和 3d 为示例性示出的 Trust Profile 的生成过程示意图。图 3a 是在图 2a 的基础上, 对 Trust Profile 的生成过程进行具体说明。图 3d 是在图 3c 的基础上, 对 Trust Profile 的生成过程进行具体说明。应该理解的是, 本申请对哈希计算采用的哈希算法不作限制。

S301, 获取第一媒体内容。

示例性地, S301 可以参照上述 S201 的描述, 在此不再赘述。

S302, 对第一媒体内容进行哈希计算, 得到第一媒体哈希值。

示例性地, 可以采用哈希算法对第一媒体内容进行哈希计算, 得到第一媒体哈希值。应该理解的是, 本申请对 S302 采用的哈希算法不作限制。

示例性地, 如图 3d 所示, 可以将第一媒体内容的初始信息和第一媒体哈希值封装在一起, 得到信任

指标 (Trust Indicators)。Trust Indicators 可以是与第一媒体内容本身相关的信息, 可以用于证实第一媒体内容的真实性。

S303, 至少根据第一媒体内容的初始信息和第一媒体哈希值进行哈希计算, 得到第一组合哈希值。

5 示例性地, S303, 根据第一媒体内容的初始信息和第一媒体哈希值进行哈希计算, 得到第一组合哈希值。

示例性地, 可以将第一媒体内容的初始信息和第一媒体哈希值进行组合 (也可以叫做连接或级联); 采用哈希算法对组合后的第一媒体内容的初始信息和第一媒体哈希值进行哈希计算, 得到第一组合哈希值。也就是说, 第一组合哈希值为第一媒体内容的初始信息和第一媒体哈希值组合的哈希值。

10 示例性地, 如图 3d 所示, 可以先可以采用哈希算法对第一媒体内容的初始信息和第一媒体内容分别进行哈希计算, 得到第一媒体内容的哈希值和第一媒体哈希值的哈希值 (Media Hash 0.Hash), 然后至少基于第一媒体内容的初始信息的哈希值和第一媒体哈希值的哈希值 (Media Hash 0.Hash) 的组合计算得到第一组合哈希值。

示例性地, 当初始信息包括多种信息时, 可以先将各种初始信息组合后再与第一媒体哈希值组合。

应该理解的是, 本申请对 S303 采用的哈希算法不作限制。

15 S304, 采用第一私钥对第一组合哈希值进行数字签名, 得到第一组合哈希值的数字签名。

一种可能的方式中, 第一私钥可以是第一用户的私钥, 即第一私钥与第一用户对应。

一种可能的方式中, 第一私钥可以是第一电子设备的私钥, 即第一私钥与第一电子设备对应。

示例性地, 可以基于数字签名算法, 采用第一私钥对第一组合哈希值进行数字签名, 得到第一组合哈希值的数字签名。应该理解的是, 本申请对 S304 采用的数字签名算法不作限制。

20 S305, 至少封装第一媒体内容的初始信息、第一媒体哈希值和第一组合哈希值的数字签名, 得到信任声明 (Trust Declaration)。

示例性地, 如图 3a 所示, 可以至少将第一媒体内容的初始信息、第一媒体哈希值和第一组合哈希值的数字签名, 得到信任声明 (Trust Declaration)。

25 示例性地, 如图 3d 所示, 可以至少将 Trust Indicators、第一媒体内容的初始信息的哈希值、第一媒体哈希值的哈希值和第一组合哈希值的数字签名封装在一起, 得到 Trust Declaration。

示例性地, 如图 3a 所示, 可以至少将第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名封装在一起, 得到 Trust Declaration。

示例性地, 如图 3d 所示, 可以至少将 Trust Indicators、第一媒体内容的初始信息的哈希值、第一媒体哈希值的哈希值、第一组合哈希值和第一组合哈希值的数字签名封装在一起, 得到 Trust Declaration。

30 S306, 至少封装 Trust Declaration, 得到第一媒体内容的 Trust Profile。Trust Profile 中还可以包括其他的修改信息, 比如, 信任记录 (Trust Record 或 Trust Manifest)。

图 3b 为示例性示出的 Trust Profile 示意图。

在图 3b 中, 第一媒体内容的 Trust Profile 可以包括 Trust Declaration, Trust Declaration 可以包括初始信息 (包括 Content ID、AIGC、Creation Info)、Media Hash 0、Hash (TD) 和 Signaturesk0。需要说明的是, 第一媒体内容的 Trust Profile 中的 Hash (TD) 为可选的数据, 也就是说, 第一媒体内容的 Trust Profile 可以包括 Trust Declaration, Trust Declaration 可以包括初始信息 (包括 Content ID、AIGC、Creation Info)、Media Hash 0 和 Signaturesk0。

在图 3b 中, 各种初始信息和 Media Hash 0 可以封装在一起。应该理解的是, 一些可能的方式中, 仅各种初始信息封装在一起。

40 应该理解的是, 图 3b 仅是本申请的一个示例, Trust Declaration 中初始信息 (Content ID、AIGC、Creation Info)、Media Hash 0、Hash (TD) 和 Signaturesk0 的位置或排列顺序可以按照需求设置, 本申请对此不作限制。

图 3c 为示例性示出的 Trust Profile 示意图。

45 在图 3c 中, Trust Declaration 可以包括 Trust Indicators、第一媒体内容的初始信息的哈希值 (例如, Media Type.Hash、AIGC.Hash)、第一媒体哈希值的哈希值和 Signaturesk0。Trust Indicators 可以包括初始信息 (例如, Content ID、Media Type、AIGC、Creation Info) 和 Media Hash 0。示例性地, Trust Declaration 还可以包括 Hash (TD)。

示例性地, 第一媒体内容的初始信息的哈希值和第一媒体哈希值的哈希值可以封装在一起。

图 3e 为示例性示出的 Trust Profile 示意图。

示例性地，在图 3e 中，Trust Declaration 可以包括 Trust Indicators、第一媒体内容的初始信息的哈希值（例如，Media Type.Hash、AIGC.Hash）、第一媒体哈希值的哈希值和 Signaturesk0。示例性地，Trust Declaration 还可以包括第一组合哈希值 Hash（TD）。

5 示例性地，在图 3e 中，第一媒体内容的元数据还可以包括第一统一资源定位符（URL，Uniform Resource Locator），第一 URL 指示第一媒体内容的初始信息或第一媒体哈希值在第一媒体内容的元数据中的位置。例如，URL1 是第一媒体哈希值在第一媒体内容的元数据中的位置，URL2 是 Media Type 在第一媒体内容的元数据中的位置，URL3 是 AIGC 在第一媒体内容的元数据中的位置。

10 示例性地，可以将第一媒体哈希值的哈希值、第一媒体内容的初始信息的哈希值和第一 URL 封装在一起。

示例性地，第一媒体内容的元数据还可以包括其它信息，其它信息可以是不用于证实第一媒体内容的真实性的信息。例如：文件名、哈希算法的名称，哈希算法用于计算得到上述实施例中提到的哈希值。

示例性地，第一组合哈希值可以是第一媒体内容的初始信息的哈希值、第一媒体哈希值的哈希值和第一 URL 组合后的哈希值。示例性地，第一组合哈希值可以是第一媒体内容的初始信息的哈希值、第一媒体哈希值的哈希值、第一 URL 和其它信息组合后的哈希值。

一种可能的场景中，在第一电子设备生成第一媒体内容的 Trust Profile 之后，第一用户可以在第一电子设备中针对第一媒体内容执行编辑操作，或者不对第一媒体内容执行编辑操作，而是在第一媒体内容的元数据进行修改（如在第一媒体内容的 Trust Profile 中添加信息）。

20 一种可能的场景中，在第一电子设备生成第一媒体内容的 Trust Profile 之后，第一电子设备将第一媒体内容和第一媒体内容的 Trust Profile 发送给第二电子设备。这样，第二用户可以在第二电子设备中对第一媒体内容执行编辑操作，或者不对第一媒体内容执行编辑操作，而是在第一媒体内容的元数据进行修改（如在第一媒体内容的 Trust Profile 中添加信息）。

示例性地，可以将根据编辑操作对第一媒体内容进行编辑处理之后得到的媒体内容，或者，对第一媒体内容的元数据进行修改后得到的媒体内容，或者，待转发（或分享）的第一媒体内容，称为第二媒体内容。然后可以在第一媒体内容的 Trust Profile 基础上，生成第二媒体内容的 Trust Profile。

25 类似地，在第二电子设备生成第二媒体内容的 Trust Profile 之后，第二用户可以在第二电子设备中对第二媒体内容执行编辑操作，或者不对第二媒体内容执行编辑操作，而是在第二媒体内容的元数据进行修改（如在第二媒体内容的 Trust Profile 中添加信息）。

30 一种可能的场景中，在第二电子设备生成第二媒体内容的 Trust Profile 之后，第二电子设备将第二媒体内容和第二媒体内容的 Trust Profile 发送给第三电子设备。这样，第三用户可以在第三电子设备中对第二媒体内容执行编辑操作，或者不对第二媒体内容执行编辑操作，而是在第二媒体内容的元数据进行修改（如在第二媒体内容的 Trust Profile 中添加信息）。

示例性地，可以将对第二媒体内容进行编辑处理之后得到的媒体内容，或者，对第二媒体内容的元数据进行修改所得到的媒体内容，或者，待转发（或分享）的第二媒体内容，称为第三媒体内容。然后可以在第二媒体内容的 Trust Profile 的基础上，生成第三媒体内容的 Trust Profile。

35 依次类推，可以将对第 N 媒体内容进行编辑处理之后得到的媒体内容，或者，对第 N 媒体内容的元数据进行修改所得到的媒体内容，或者，待转发（或分享）的第 N 媒体内容，称为第 N+1 媒体内容。然后可以在第 N 媒体内容的 Trust Profile 基础上，生成第 N+1 媒体内容的 Trust Profile；可以参照如下图 4a 至图 8a 实施例中的描述。

40 需要说明的是，图 4a 至图 8a 实施例，当 N=1 时，第一媒体内容可以是指图 2a 实施例或图 3a 实施例中的第一媒体内容。

应该理解的是，第 N 并不构成对具体数量的限制，只是为了便于区分。一些可能情况中，第 N 媒体内容和第 N+1 媒体内容，可以是按照时间顺序产生的媒体内容；例如，N=2 时，第三媒体内容是在第二媒体内容之后产生的。也就是说，一些可能的情况中，第 N 和第 N+1 可以用于表示顺序。图 4a 为示例性示出的 Trust Profile 的生成过程示意图。

45 S401，获取第 N+1 媒体内容，第 N+1 媒体内容基于第 N 媒体内容得到。

一种可能的方式中，当第 N 用户期望在第 N 媒体内容的 Trust Profile 中添加信息时，第 N 用户可以在第 N 电子设备中进入第 N 媒体内容对应的 Trust Profile 添加界面，此时，第 N 电子设备可以获取第 N 媒

体内容作为第 N+1 媒体内容（即第 N+1 媒体内容为第 N 媒体内容），然后执行 S402。

一种可能的方式中，当第 N 用户针对第 N 媒体内容执行转发操作后，第 N 电子设备可以获取第 N 媒体内容作为第 N+1 媒体内容，然后执行 S402；待生成第 N+1 媒体内容的 Trust Profile 之后，再转发第 N+1 媒体内容和第 N+1 媒体内容的 Trust Profile。

- 5 一种可能的方式中，当第 N+1 用户期望对第 N 媒体内容进行编辑时，可以在第 N+1 电子设备中进入第 N 媒体内容对应的编辑界面，然后执行编辑操作；对应的，第 N+1 电子设备可以响应于编辑操作对第 N 媒体内容进行编辑处理。待第 N+1 用户完成对第 N 媒体内容的编辑后，第 N+1 电子设备即可得到第 N+1 媒体内容；即第 N+1 媒体内容为对第 N 媒体内容编辑处理得到的媒体内容。

- 其中，当第 N 媒体内容为图像/视频时，编辑处理可以包括但不限于：裁剪、旋转、调色、添加文本、删除文本/目标对象等，本申请对此不作限制。当第 N 媒体内容为音频时，编辑处理可以包括但不限于：裁剪、加速、减速、升调、降调等，本申请对此不作限制。当第 N 媒体内容为图形时，编辑处理可以包括但不限于：裁剪、旋转、调色、添加线条等，本申请对此不作限制。当第 N 媒体内容为文本时，编辑处理可以包括但不限于：添加文本、删除文本、文本顺序调换、字体大小等，本申请对此不作限制。

- 10 如图 4c 所示，生成第 N+1 媒体内容的元数据，第 N+1 媒体内容的元数据包括第一媒体内容的初始信息和第一数据的数字签名；所述 N+1 媒体内容的元数据还包括 N 个媒体哈希值，其中，第一媒体哈希值是所述第一媒体内容的哈希值，第 N+1 媒体哈希值是所述第 N+1 媒体内容的哈希值，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据；N 为正整数。

- 示例性地，S402，生成第 N+1 媒体内容的元数据，第 N+1 媒体内容的元数据包括第一媒体内容的初始信息和第一组合哈希值的数字签名；N+1 媒体内容的元数据还包括 N+1 个媒体哈希值，其中，第一媒体哈希值是所述第一媒体内容的哈希值，第 N+1 媒体哈希值是第 N+1 媒体内容的哈希值，第一组合哈希值是根据初始信息和第一媒体哈希值确定的，N 为正整数。

示例性地，S402 生成的第 N+1 媒体内容的元数据，可以是指第 N+1 媒体内容的 Trust Profile。

示例性地，可以由第 N+1 电子设备/第 N 电子设备生成第 N+1 媒体内容的 Trust Profile。

- 20 示例性地，可以对第 N+1 媒体内容进行哈希计算，得到第 N+1 媒体哈希值。由于第 N+1 电子设备在获取第 N+1 媒体内容的同时，可以获取到第 N 媒体内容的 Trust Profile，进而第 N+1 电子设备可以基于第 N 媒体内容的 Trust Profile 和第 N+1 媒体哈希值，生成第 N+1 媒体内容的 Trust Profile。

需要说明的是，无论第 N 用户在第 N 媒体内容对应的 Trust Profile 添加界面是否执行信息添加操作，第 N+1 电子设备均会执行 S402。

- 30 应该理解的是，当 N=1 时，根据图 2a 和图 3a 实施例的描述可知，获取到的第一媒体内容的 Trust Profile 包括 1 个媒体哈希值，即第一媒体哈希值。在执行 S402 后，得到的第二媒体内容的 Trust Profile 可以包括 2 个媒体哈希值：第一媒体哈希值和第二媒体哈希值。

当 N=2 时，获取到的第二媒体内容的 Trust Profile 包括 2 个媒体哈希值：第一媒体哈希值和第二媒体哈希值。在执行 S402 后，得到的第三媒体内容的 Trust Profile 可以包括 3 个媒体哈希值：第一媒体哈希值、第二媒体哈希值和第三媒体哈希值。

- 35 也就是说，获取到的第 N 媒体内容的 Trust Profile 可以包括 N 个媒体哈希值，生成的第 N+1 媒体内容的 Trust Profile 可以包括 N+1 个媒体哈希值，第 N+1 媒体哈希值是第 N+1 媒体内容的哈希值。

应该理解的是，当第 N+1 媒体内容为第 N 媒体内容时，第 N+1 媒体哈希值与第 N 媒体哈希值相同。

图 4b 为示例性示出的 Trust Profile 示意图。

- 40 示例性地，在图 4b 中，第 N+1 媒体内容的 Trust Profile 可以包括：Content ID（即第一媒体内容的数字内容标识）、AIGC（即 AIGC 标识）、Creation Info（即 Creation Information，可以包括生第一媒体内容的成时间、第一媒体内容的作者名称、第一媒体内容的生成地点等）、Media Hash 0（即第一媒体哈希值）、Signaturesk0（即第一组合哈希值的数字签名）、Media Hash 1（即第二媒体哈希值）、Media Hash 2（即第三媒体哈希值）、.....、Media Hash N（即第 N+1 媒体哈希值）。示例性地，第 N+1 媒体内容的 Trust Profile 还可以包括 Hash（TD）（即第一组合哈希值）。

- 45 应该理解的是，图 4b 仅是本申请的一个示例，Trust Profile 中各种信息的位置或排列顺序可以按照需求设置，本申请对此不作限制。

示例性地，还可以在生成第 N+1 媒体内容的 Trust Profile 的过程中，将第 N 组合哈希值和第 N+1 媒体哈希值进行关联以及数字签名，以防止 Trust Profile 中的部分信息被伪造；具体可以参照图 5a 实施例中

的描述。

图 5a 或 5b 为示例性示出了 Trust Profile 的生成过程示意图。

S501, 获取第 N+1 媒体内容, 第 N+1 媒体内容基于第 N 媒体内容得到。

S502, 对第 N+1 媒体内容进行哈希计算, 得到第 N+1 媒体哈希值。

5 示例性地, 可以采用哈希算法对第 N+1 媒体内容进行哈希计算, 得到第 N+1 媒体哈希值。应该理解的是, 本申请对 S502 采用的哈希算法不作限制。

如图 5a 所示, S503, 根据第 N 组合哈希值和第 N+1 媒体哈希值, 确定第 N+1 组合哈希值。示例性地, 可以对第 N 组合哈希值和第 N+1 媒体哈希值进行组合, 然后采用哈希算到对组合后的第 N 组合哈希值和第 N+1 媒体哈希值进行哈希计算, 得到第 N+1 组合哈希值。也就是说, 在 S503 中, 第 N+1 组合哈希值是第 N 组合哈希值和第 N+1 媒体哈希值组合的哈希值。

如图 5b 所示, S503, 根据第 N 组合哈希值、第 N 组合哈希值的数字签名和第 N+1 媒体哈希值, 确定第 N+1 组合哈希值。示例性地, 可以对第 N 组合哈希值、第 N 组合哈希值的数字签名和第 N+1 媒体哈希值进行组合, 然后采用哈希算到对组合后的第 N 组合哈希值、第 N 组合哈希值的数字签名和第 N+1 媒体哈希值进行哈希计算, 得到第 N+1 组合哈希值。也就是说, 在 S503 中, 第 N+1 组合哈希值是第 N 组合哈希值、第 N 组合哈希值的数字签名和第 N+1 媒体哈希值组合的哈希值。

应该理解的是, 本申请对 S503 采用的哈希算法不作限制。

S504, 采用第 N+1 私钥对第 N+1 组合哈希值进行数字签名, 得到第 N+1 组合哈希值的数字签名。

一种可能的方式中, 第 N+1 私钥可以是第 N+1 用户的私钥, 即第 N+1 私钥与第 N+1 用户对应。

一种可能的方式中, 第 N+1 私钥可以是第 N+1 电子设备的私钥, 即第 N+1 私钥与第 N+1 电子设备对应。

需要说明的是, N+1 个私钥中的任意两个私钥可以相同也可以不同, 具体可以根据生成 Trust Profile 的用户和电子设备确定, 本申请对此不作限制。

示例性地, 本申请可以基于数字签名算法, 采用第 N+1 私钥对第 N+1 组合哈希值进行数字签名, 得到第 N+1 组合哈希值的数字签名。应该理解的是, 本申请对 S504 涉及的数字签名算法不作限制。

25 S505, 至少将第 N+1 媒体哈希值和第 N+1 组合哈希值的数字签名, 添加至第 N 媒体内容的 Trust Profile 中, 得到第 N+1 媒体内容的 Trust Profile。示例性地, 还可以将第 N+1 组合哈希值添加至第 N 媒体内容的 Trust Profile 中, 得到第 N+1 媒体内容的 Trust Profile。

应该理解的是, 当 N=1 时, 根据图 2a 和图 3a 实施例的描述可知, 获取到的第一媒体内容的 Trust Profile 包括 1 个媒体哈希值 (即第一媒体哈希值)、1 个组合哈希值 (即第一组合哈希值) 和 1 个组合哈希值的数字签名 (即第一组合哈希值的数字签名)。执行 S502~505 之后, 得到的第二媒体内容的 Trust Profile 可以包括 2 个媒体哈希值 (包括第一媒体哈希值和第二媒体哈希值)、2 个组合哈希值 (包括第一组合哈希值和第二组合哈希值) 和 2 个组合哈希值的数字签名 (即第一组合哈希值的数字签名和第二组合哈希值的数字签名)。

35 当 N=2 时, 获取到的第二媒体内容的 Trust Profile 包括 2 个媒体哈希值、2 个组合哈希值和 2 个组合哈希值的数字签名。执行 S502~505 之后, 得到的第三媒体内容的 Trust Profile 可以包括 3 个媒体哈希值 (包括第一媒体哈希值、第二媒体哈希值和第三媒体哈希值)、3 个组合哈希值 (包括第一组合哈希值、第二组合哈希值和第三组合哈希值) 和 3 个组合哈希值的数字签名 (即第一组合哈希值的数字签名、第二组合哈希值的数字签名和第三组合哈希值的数字签名)。

也就是说, 获取到的第 N 媒体内容的 Trust Profile 可以包括 N 个媒体哈希值、N 个组合哈希值和 N 个组合哈希值的数字签名, 进而生成的第 N+1 媒体内容的 Trust Profile 可以包括 N+1 个媒体哈希值、N+1 个组合哈希值以及 N+1 个组合哈希值的数字签名。

需要说明的是, 无论第 N 用户在第 N 媒体内容对应的 Trust Profile 添加界面是否执行信息添加操作, 第 N+1 电子设备均会执行 S502~S505。

图 5c 为示例性示出的 Trust Profile 示意图。

45 在图 5c 中, 第 N+1 媒体内容的 Trust Profile 可以包括: Content ID (即第一媒体内容的数字内容标识)、AIGC (即 AIGC 标识)、Creation Info (即 Creation Information, 可以包括生第一媒体内容的成时间、第一媒体内容的作者名称、第一媒体内容的生成地点等)、Media Hash 0 (即第一媒体哈希值)、Hash (TD) (即第一组合哈希值)、Signaturesk0 (即第一组合哈希值的数字签名)、Media Hash 1 (即第二媒体哈希

值)、MTR1(即第二组合哈希值)和 Signaturesk1(MTR1)(即第二组合哈希值的数字签名)、.....、Media Hash N(即第 N+1 媒体哈希值)、MTR N(即第 N+1 组合哈希值)和 SignatureskN(MTR N)(即第 N+1 组合哈希值的数字签名)。

应该理解的是,图 5c 仅是本申请的一个示例,Trust Profile 中各种信息的位置或排列顺序可以按照需求设置,本申请对此不作限制。

示例性地,还可以生成针对第 N+1 媒体内容的声明(Claim)和针对第二媒体内容的声明的哈希值,并将第 N+1 媒体内容的声明(Claim)和针对第二媒体内容的声明的哈希值,作为第 N+1 媒体内容的 Trust Profile 的一部分。可以参照图 6a 实施例的描述。

图 6a 或图 6b 为示例性示出的 Trust Profile 生成过程示意图。

10 S601, 获取第 N+1 媒体内容,第 N+1 媒体内容基于第 N 媒体内容得到。

S602, 获取一个或多个第 N+1 媒体声明和一个或多个第 N+1 声明哈希值。

一种可能的方式中,在第 N 用户在第 N 媒体内容对应的 Trust Profile 添加界面中,执行针对第 N+1 媒体内容的声明添加操作后,第 N 电子设备可以获取到针对第 N+1 媒体内容的一个或多个声明(后续可以称为第 N+1 媒体声明)。其中,第 N+1 媒体声明可以包括版权信息,缩略图、是否可以被修改,操作权限、使用权限、第 N+1 媒体内容的来源等,本申请对此不作限制。

举个例子,假设第 N+1 媒体内容为图像,则针对第 N+1 媒体内容的一个或多个第 N+1 媒体声明可以如:对第 N+1 媒体内容中不可更改区域的声明、对第 N+1 媒体内容中不可更改对象的声明、对第 N+1 媒体内容的操作权限的声明、对第 N+1 媒体内容使用权限的说明等等。

一种可能的方式中,在第 N 用户针对第 N 媒体内容执行转发操作后,第 N 用户还可以进入第 N 媒体内容对应的 Trust Profile 添加界面中,执行针对第 N+1 媒体内容的声明添加操作;这样,第 N+1 电子设备可以获取到针对第 N+1 媒体内容的一个或多个第 N+1 媒体声明。其中,第 N+1 媒体声明可以包括版权信息,缩略图、是否可以被修改,操作权限、使用权限、第 N+1 媒体内容的来源等,本申请对此不作限制。

一种可能的方式中,当第 N+1 媒体内容为对第 N 媒体内容进行编辑处理得到的时,第 N+1 电子设备在响应于第 N+1 用户针对第 N 媒体内容执行的编辑操作,对第 N 媒体内容进行编辑处理的过程中,可以记录编辑处理参数。在获取到第 N+1 媒体内容之后,可以根据记录的编辑处理参数,生成针对第 N+1 媒体内容的一个或多个第 N+1 媒体声明。

其中,第 N+1 媒体声明可以包括编辑信息。举个例子,假设第 N+1 媒体内容为图像,则针对第 N+1 媒体内容的一个或多个第 N+1 媒体声明如旋转参数、裁剪参数等等。

应该理解的是,当第 N+1 媒体内容为对第 N 媒体内容进行编辑处理得到的时,第 N+1 用户在执行完针对第 N 媒体内容的编辑操作之后,也可以在第 N+1 电子设备中进入第 N+1 媒体内容对应的 Trust Profile 添加界面中,执行针对第 N+1 媒体内容的声明添加操作;这样,第 N+1 电子设备可以获取到针对第 N+1 媒体内容的一个或多个第 N+1 媒体声明。此时,第 N+1 媒体声明可以包括版权信息,缩略图、是否可以被修改,操作权限、使用权限、第 N+1 媒体内容的来源等,本申请对此不作限制。

示例性地,针对每一条第 N+1 媒体声明,可以采用哈希算法对该条第 N+1 媒体声明进行哈希计算,得到该条第 N+1 媒体声明的第 N+1 声明哈希值。应该理解的是,本申请对 S602 采用的哈希算法不做限制。

应该理解的是,S602 为可选步骤,也就是说,可以在生成 Trust Profile 的过程中,针对第 N+1 媒体内容进行声明,也可以不对第 N+1 媒体内容进行声明;这样,可以增加 Trust Profile 的灵活性和向后兼容能力。

40 S603, 对第 N+1 媒体内容进行哈希计算,得到第 N+1 媒体哈希值。

如图 6a 所示,S604,根据第 N 组合哈希值、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值,确定第 N+1 组合哈希值。

示例性地,可以将第 N 组合哈希值、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中的一个或多个哈希值连接后进行哈希计算,得到中间哈希值。

45 当中间哈希值是采用第 N 组合哈希值、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中所有哈希值连接后进行哈希计算得到的,则可以将中间哈希值作为第 N+1 组合哈希值。

如图 6b 所示,S604,根据第 N 组合哈希值、第 N 组合哈希值的数字签名、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值,确定第 N+1 组合哈希值。

示例性地, 可以将第 N 组合哈希值、第 N 组合哈希值的数字签名、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中的一个或多个哈希值连接后进行哈希计算, 得到中间哈希值。

当中间哈希值是采用第 N 组合哈希值、第 N 组合哈希值的数字签名、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中所有哈希值连接后进行哈希计算得到的, 则可以将中间哈希值作为第 N+1 组合哈希值。

图 6c 或图 6d 为示例性示出的第 N+1 组合哈希值生成过程示意图。在图 6c 或 6d 中,  $N=1$ , 第二声明哈希值的数量为 3, 3 个第二声明哈希值分别为: Claim Hash 21、Claim Hash 22 和 Claim Hash 23。

假设, 第一组合哈希值为 Hash (TD), 第一组合哈希值的数字签名为 Signature sk0, 第二媒体哈希为 Media Hash 1。在图 6c 中, 可以将 Hash (TD)、Media Hash 1 和 Claim Hash 21、Claim Hash 22、Claim Hash 23、连接之后进行哈希计算, 得到第二组合哈希值 MTR1; 在图 6d 中, 可以将 Hash (TD)、Signature sk0、Media Hash 1 和 Claim Hash 21、Claim Hash 22、Claim Hash 23、连接之后进行哈希计算, 得到第二组合哈希值 MTR1。应该理解的是, 本申请不限制 Claim Hash 21、Claim Hash 22、Claim Hash 23、Signature sk0、Hash (TD) 和 Media Hash 1 的连接顺序。

如图 6c 所示, 当中间哈希值是采用第 N 组合哈希值、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中部分哈希值连接后进行哈希计算得到的, 则可以根据中间哈希值与第 N 组合哈希值、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中另一部分哈希值进行哈希计算, 得到第 N+1 组合哈希值。示例性地, 可以采用哈希树, 对第 N 组合哈希值、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值进行哈希计算, 得到第 N+1 组合哈希值。

如图 6d 所示, 当中间哈希值是采用第 N 组合哈希值、第 N 组合哈希值的数字签名、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中部分哈希值连接后进行哈希计算得到的, 则可以根据中间哈希值与第 N 组合哈希值、第 N 组合哈希值的数字签名、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中另一部分哈希值进行哈希计算, 得到第 N+1 组合哈希值。示例性地, 可以采用哈希树, 对第 N 组合哈希值、第 N 组合哈希值的数字签名、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值进行哈希计算, 得到第 N+1 组合哈希值。

其中, 哈希树是一种数据结构, 哈希树可以包括但不限于二叉树、三叉树、默克尔树 (Merkle Tree) 等等, 本申请对此不作限制。

一种可能的方式中, 第 N+1 组合哈希值是哈希树的根节点的值, 第 N 组合哈希值、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值分别为哈希树的叶子节点的值。

图 6e 和 6f 为示例性示出的第 N+1 组合哈希值生成过程示意图。

在图 6e 中, 哈希树为 Merkle Tree, 第 N+1 组合哈希值 (MTR N) 是默克尔树的根节点 (Merkle Tree Root, MTR) 的值, 第 N 组合哈希值 (MTR N-1)、第 N+1 媒体哈希值 (Media Hash N) 和 2 个第 N+1 声明哈希值 (Claim Hash N1 和 Claim Hash N2) 分别为 Merkle Tree 的叶子节点的值。

参照图 6e, 示例性地, 可以对连接后的 MTR N-1 和 Media Hash N 进行哈希计算, 得到 Hash X1 (也就是中间哈希值), 对连接后的 Claim Hash N1 和 Claim Hash N2 进行哈希计算, 得到 Hash X2 (也就是中间哈希值)。之后, 对连接后的 Hash X1 和 Hash X2 进行哈希计算, 得到 MTR N。

在图 6f 中, 第 N+1 组合哈希值 (MTR N) 是默克尔树的根节点 (Merkle Tree Root, MTR) 的值, 第 N 组合哈希值 (MTR N-1)、第 N 组合哈希值的数字签名 (Signature skN-1)、第 N+1 媒体哈希值 (Media Hash N) 和 2 个第 N+1 声明哈希值 (Claim Hash N1 和 Claim Hash N2) 分别为 Merkle Tree 的叶子节点的值。

参照图 6f, 示例性地, 可以对连接后的 MTR N-1 和 Signature skN-1 进行哈希计算, 得到 Hash X3 (也就是中间哈希值), 对连接后的 Claim Hash N1 和 Media Hash N 进行哈希计算, 得到 Hash X4 (也就是中间哈希值), 对连接后的 Claim Hash N2 和 Claim Hash N3 进行哈希计算, 得到 Hash X5 (也就是中间哈希值)。之后, 对连接后的 Hash X3 和 Hash X4 进行哈希计算, 得到 Hash X6, 对连接后的 Hash X5 进行哈希计算, 得到 Hash X7。之后, 对连接后的 Hash X6 和 Hash X7 进行哈希计算, 得到 MTR N。

其中, 当 N 等于 1 时, MTR 0 是指第一组合哈希值, 也就是上述的 Hash (TD)。

应该理解的是, 图 6e 或 6f 仅是 Merkle Tree 的一个示例, 本申请的 Merkle Tree 可以是其他数据结构, 本申请对此不作限制。

应该理解的是, 本申请对第 N 组合哈希值、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值对应

Merkle Tree 的哪个叶子节点不作限制。

一种可能的方式中，第 N+1 组合哈希值是哈希树的根节点的值，第 N 组合哈希值为哈希树的左子树的根节点的值，第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值分别为哈希树的右子树的叶子节点的值。

5 图 6g 或 6h 为示例性示出的第 N+1 组合哈希值生成过程示意图。

在图 6g 中，哈希树为 Merkle Tree，第 N+1 组合哈希值 (MTR N) 是 Merkle Tree 的根节点的值，第 N 组合哈希值 (MTR N-1) 为 Merkle Tree 的左子树的根节点的值，第 N+1 媒体哈希值 (Media Hash N) 和 2 个第 N+1 声明哈希值 (Claim Hash N1 和 Claim Hash N2) 分别为 Merkle Tree 的右子树的叶子节点的值。参照图 6g，示例性地，可以对连接后的 Claim Hash N1 和 Media Hash N 进行哈希计算，得到 Hash X8 (也就是中间哈希值)，对 Claim Hash N2 进行哈希计算，得到 Hash X9 (也就是中间哈希值)。之后，对连接后的 Hash X8 和 Hash X9 进行哈希计算，得到 Hash X10。随后，对连接后的 Hash X10 和 MTR N-1 进行哈希计算，得到 MTR N。

在图 6h 中，哈希树为 Merkle Tree，第 N+1 组合哈希值 (MTR N) 是 Merkle Tree 的根节点的值，Hash X14 为 Merkle Tree 的左子树的根节点的值，第 N 组合哈希值 (MTR N-1) 和第 N 组合哈希值的数字签名 (Signature skN-1) 为左子树的根节点的子节点的值，第 N+1 媒体哈希值 (Media Hash N) 和 2 个第 N+1 声明哈希值 (Claim Hash N1 和 Claim Hash N2) 分别为 Merkle Tree 的右子树的叶子节点的值。参照图 6h，示例性地，可以对连接后的 Claim Hash N1 和 Media Hash N 进行哈希计算，得到 Hash X11 (也就是中间哈希值)，对 Claim Hash N2 进行哈希计算，得到 Hash X12 (也就是中间哈希值)，可以对连接后的 MTR N-1 和 Signature skN-1 进行哈希计算，得到 Hash X14 (也就是中间哈希值)。之后，对连接后的 Hash X11 和 Hash X12 进行哈希计算，得到 Hash X13。随后，对连接后的 Hash X3 和 Hash X14 进行哈希计算，得到 MTR N。

其中，当 N 等于 1 时，MTR 0 是指第一组合哈希值，也就是上述的 Hash (TD)。

应该理解的是，本申请对第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值对应 Merkle Tree 的哪个叶子节点不作限制。

25 示例性地，当哈希树为 Merkle Tree 时，还可以为 Merkle Tree 进行剪枝，以降低 Trust Profile 占用的内存。具体地，可以将一个或多个第 N+1 媒体声明中的部分或全部第 N+1 媒体声明以及对应的第 N+1 声明哈希值删除，仅保留删除的第 N+1 声明哈希值的父节点的哈希值即可。此外，还可以对删除的第 N+1 媒体声明进行声明 (可以称为第 N+1 媒体删除声明)，并将删除的第 N+1 声明哈希值的父节点的哈希值，作为第 N+1 媒体删除声明的哈希值 (可以称为第 N+1 声明删除哈希值)。

30 例如，参照图 6e，可以删除图 6e 中的 Claim Hash N1 和 Claim Hash N2，保留 Hash X2。

S605，采用第 N+1 私钥对第 N+1 组合哈希值进行数字签名，得到第 N+1 组合哈希值的数字签名。

示例性地，应该理解的是，本申请对 S605 采用的数字签名算法不作限制。

S606，将一个或多个第 N+1 媒体声明、一个或多个第 N+1 声明哈希值、第 N+1 媒体哈希值、第 N+1 组合哈希值和第 N+1 组合哈希值的数字签名，添加至第 N 媒体内容的 Trust Profile 中，得到第 N+1 媒体内容的 Trust Profile。

应该理解的是，第一媒体内容的 Trust Profile 中不包括媒体声明和声明哈希值。

在图 6a 或 6b 的实施例中，第 N+1 媒体内容的 Trust Profile 可以包括：第一媒体内容的初始信息、N+1 个媒体哈希值和 N+1 个组合哈希值、N+1 个组合哈希值的数字签名、一个或多个第 N+1 媒体声明和一个或多个第 N+1 声明哈希值。

40 应该理解的是，当第 N 媒体内容的 Trust Profile 中包括一个或多个第 N 媒体声明和一个或多个第 N 声明哈希值时，第 N+1 媒体内容的 Trust Profile 还可以包括一个或多个第 N 媒体声明和一个或多个第 N 声明哈希值。当第 N-1 媒体内容的 Trust Profile 中包括一个或多个第 N-1 媒体声明和一个或多个第 N-1 声明哈希值时，第 N+1 媒体内容的 Trust Profile 还可以包括一个或多个第 N-1 媒体声明和一个或多个第 N-1 声明哈希值；以此类推，本申请对此不作限制。

45 图 6i 为示例性示出的 Trust Profile 示意图。

在图 6i 中，第 N+1 媒体内容的 Trust Profile 可以包括：Content ID (即第一媒体内容的数字内容标识)、AIGC (即 AIGC 标识)、Creation Info (即 Creation Information，可以包括生第一媒体内容的成时间、第一媒体内容的作者名称、第一媒体内容的生成地点等)、Media Hash 0 (即第一媒体哈希值)、Hash (TD)

(即第一组合哈希值)、Signaturesk0 (即第一组合哈希值的数字签名)、Media Hash 1 (即第二媒体哈希值)、MTR1 (即第二组合哈希值) 和 Signaturesk1 (MTR1) (即第二组合哈希值的数字签名)、Claim 21 (即第二媒体声明) 和 Claim Hash 21 (即第二声明哈希值)、Claim 22 (即第二媒体声明) 和 Claim Hash 22 (即第二声明哈希值)、Claim 23 (即第二媒体声明) 和 Claim Hash 23 (即第二声明哈希值)、.....、Media Hash N (即第 N+1 媒体哈希值)、MTR N (即第 N+1 组合哈希值) 和 SignatureskN (MTR N) (即第 N+1 组合哈希值的数字签名)、Claim N1 (即第 N+1 媒体声明) 和 Claim Hash N1 (即第 N+1 声明哈希值)。

图 6j 为示例性示出的 Trust Profile 示意图。

示例性地, 图 6j 是删除了图 6i 中所有的第二媒体声明和所有第二媒体声明的第二声明哈希值, 并增加了第二媒体删除声明 (Claim D) 和第二声明删除哈希值 (Claim Hash D) 的 Trust Profile 示意图。图 6j 中其他信息可以参照图 6i 中的描述, 在此不再赘述。

应该理解的是, 图 6i 和图 6j 仅是本申请的一个示例, Trust Profile 中各种信息的位置或排列顺序可以按照需求设置, 本申请对此不作限制。

示例性地, 可以将第 N+1 媒体哈希值、第 N+1 组合哈希值、第 N+1 个组合哈希值的数字签名进行封装, 得到第 N+1 媒体内容的 Trust Profile。

图 7a 或 7b 为示例性示出的 Trust Profile 的生成过程示意图。图 7a 是在图 5a 的基础上进行的说明, 图 7b 是在图 5b 的基础上进行的说明。

S701, 获取第 N+1 媒体内容, 第 N+1 媒体内容基于第 N 媒体内容得到。

S702, 对第 N+1 媒体内容进行哈希计算, 得到第 N+1 媒体哈希值。

S703, 根据第 N 组合哈希值和第 N+1 媒体哈希值, 确定第 N+1 组合哈希值。

S704, 采用第 N+1 私钥对第 N+1 组合哈希值进行数字签名, 得到第 N+1 组合哈希值的数字签名。

S705, 将第 N+1 媒体哈希值、第 N+1 组合哈希值和第 N+1 组合哈希值的数字签名封装以得到第 N+1 媒体内容的信任记录 (Trust Record 或 Trust Manifest)。

其中, 第 N+1 媒体内容的信任记录, 可以采用 Trust Record N 表示。例如, 当 N 等于 1 时, 第二媒体内容的 Trust Record 可以采用 Trust Record 1 表示。

示例性地, 可以将第 N+1 媒体哈希值、第 N+1 组合哈希值和第 N+1 组合哈希值的数字签名封装在一起, 得到 Trust Record N。

S706, 将 Trust Record N 添加至第 N 媒体内容的 Trust Profile 中, 得到第 N+1 媒体内容的 Trust Profile。

应该理解的是, 当第 N 媒体内容的 Trust Profile 中的信息未被封装成 Trust Declaration、Trust Record 1、.....、Trust Record N-1 时, 则在 S706 之前, 还可以将第 N 媒体内容的 Trust Profile 中的信息装成 Trust Declaration、Trust Record 1、.....、Trust Record N-1; 然后, 可以将 Trust Declaration、Trust Record 1、.....、Trust Record N-1, 封装成为第 N 媒体内容的 Trust Profile。之后, 可以将 Trust Record N 添加至第 N 媒体内容的 Trust Profile 中, 得到第 N+1 媒体内容的 Trust Profile。需要说明的是, 将 Trust Record N 添加至第 N 媒体内容的 Trust Profile 中, 可以理解成将 Trust Record N 与 Trust Declaration、Trust Record 1、.....、Trust Record N-1 封装在一起, 得到第 N+1 媒体内容的 Trust Profile。

其中, 将第 N 媒体内容的 Trust Profile 中的信息装成 Trust Declaration 的过程, 可以参照上述实施例的描述; 以及将第 N 媒体内容的 Trust Profile 中的信息装成 Trust Record 1、.....、Trust Record N-1 的过程, 可以参照 S705 的描述, 在此不再赘述。

图 7c 为示例性示出的 Trust Profile 示意图。

在图 7c 中, 第 N+1 媒体内容的 Trust Profile 可以包括 Trust Declaration、Trust Record 1、.....、Trust Record N。其中, Trust Record 1 可以包括: 第二媒体哈希值 (Media Hash 1)、第二组合哈希值 (MTR1) 和第二组合哈希值的数字签名 (Signaturesk1 (MTR1))。Trust Record N 可以包括: Media Hash N (即第 N+1 媒体哈希值)、MTR N (即第 N+1 组合哈希值) 和 SignatureskN (MTR N) (即第 N+1 组合哈希值的数字签名)。

应该理解的是, 图 7c 仅是本申请的一个示例, Trust Profile 中各种信息的位置或排列顺序可以按照需求设置, 本申请对此不作限制。

示例性地, 可以将第 N+1 媒体哈希值和第 N+1 组合哈希值、第 N+1 个组合哈希值的数字签名、一个或多个第 N+1 媒体声明和一个或多个第 N+1 声明哈希值进行封装, 得到第 N+1 媒体内容的 Trust Profile。

图 8a 或 8b 为示例性示出的 Trust Profile 的生成过程示意图。图 8a 是在图 6a 的基础上进行的说明，图 8b 是在图 6b 的基础上进行的说明。

S801, 获取第 N+1 媒体内容, 第 N+1 媒体内容基于第 N 媒体内容得到。

S802, 获取一个或多个第 N+1 媒体声明和一个或多个第 N+1 声明哈希值。

5 S803, 对第 N+1 媒体内容进行哈希计算, 得到第 N+1 媒体哈希值。

S804, 根据第 N 组合哈希值、第 N+1 媒体哈希值和一个或多个第 N+1 声明哈希值, 确定第 N+1 组合哈希值。

S805, 采用第 N+1 私钥对第 N+1 组合哈希值进行数字签名, 得到第 N+1 组合哈希值的数字签名。

10 S806, 将第 N+1 媒体哈希值、第 N+1 组合哈希值、第 N+1 组合哈希值的数字签名、一个或多个第 N+1 媒体声明和一个或多个第 N+1 声明哈希值封装, 以得到 Trust Record N。

S807, 将 Trust Record N 添加至第 N 媒体内容的 Trust Profile 中, 得到第 N+1 媒体内容的 Trust Profile。

15 应该理解的是, 当第 N 媒体内容的 Trust Profile 中的信息未被封装成 Trust Declaration、Trust Record 1、.....、Trust Record N-1; 则在 S807 之前, 还可以将第 N 媒体内容的 Trust Profile 中的信息装成 Trust Declaration、Trust Record 1、.....、Trust Record N-1; 然后将 Trust Record N 添加至第 N 媒体内容的 Trust Profile 中, 得到第 N+1 媒体内容的 Trust Profile。

其中, 将第 N 媒体内容的 Trust Profile 中的信息装成 Trust Declaration 的过程, 可以参照上述实施例的描述; 以及将第 N 媒体内容的 Trust Profile 中的信息装成 Trust Record 1、.....、Trust Record N-1 的过程, 可以参照 S806 的描述, 在此不再赘述。

图 8c 为示例性示出的 Trust Profile 示意图。

20 在图 8c 中, 第 N+1 媒体内容的 Trust Profile 可以包括 Trust Declaration、Trust Record 1、.....、Trust Record N。其中, Trust Record 1 可以包括: Media Hash 1 (即第二媒体哈希值)、MTR1 (即第二组合哈希值) 和 Signaturesk1 (MTR1) (即第二组合哈希值的数字签名)、Claim 21 (即第二媒体声明) 和 Claim Hash 21 (即第二声明哈希值)、Claim 22 (即第二媒体声明) 和 Claim Hash 22 (即第二声明哈希值)、Claim 23 (即第二媒体声明) 和 Claim Hash 23 (即第二声明哈希值)。Trust Record N 可以包括: Media Hash N (即第 N+1 媒体哈希值)、MTR N (即第 N+1 组合哈希值) 和 SignatureskN (MTR N) (即第 N+1 组合哈希值的数字签名)、Claim N1 (即第 N+1 媒体声明) 和 Claim Hash N1 (即第 N+1 声明哈希值)。

25 应该理解的是, 图 8c 仅是本申请的一个示例, Trust Profile 中各种信息的位置或排列顺序可以按照需求设置, 本申请对此不作限制。

图 8d 为示例性示出的 Trust Profile 示意图。

30 在图 8d 中, Trust Profile 可以包括 Trust Manifest 和第二数字签名, 第二数字签名是第二数据的数字签名, Trust Manifest 可以包括修改声明 Assertions, Assertions 可以包括第 N+1 媒体哈希值和第 N+1 声明, 第二数据可以是至少基于第 N+1 媒体哈希值和第 N+1 声明确定的数据。示例性地, 可以至少将第 N+1 媒体哈希值和第 N+1 声明封装形成 Assertions。

35 示例性地, 第二数据是至少由第 N+1 媒体哈希值和第 N+1 声明组合后的数据, 或者, 第一数据是至少由第 N+1 声明的哈希值和第 N+1 媒体哈希值的哈希值组合后的数据。

40 示例性地, 第二数据也可第 N+1 组合哈希值, 第 N+1 组合哈希值包括第 N+1 声明和第 N+1 媒体哈希值的哈希值组合后的哈希值。示例性地, 第 N+1 组合哈希值包括第 N+1 声明、第 N+1 媒体哈希值的哈希值组合后的哈希值和其它描述性信息组合后的哈希值, 其它描述性信息可以不是第 N+1 声明中的其他描述性信息, 例如, 生成 Trust Manifest 的工具的信息或者其它描述第 N+1 声明的信息, 本申请对此不作限制。

示例性地, 第二数据也可第 N+1 组合哈希值, 第 N+1 组合哈希值可以包括第 N+1 声明的哈希值和第 N+1 媒体哈希值的哈希值 (例如, 第二媒体哈希值 Media Hash 1. Hash) 组合后的哈希值。示例性地, 第二组合哈希值是第 N+1 声明的哈希值、第 N+1 媒体哈希值的哈希值和其它元数据信息的哈希值组合后的哈希值。

45 示例性地, 在图 8d 中, 第 N+1 媒体内容的元数据还可以包括第 N+1 媒体哈希值的哈希值和第 N+1 声明的哈希值。示例性地, 可以将第 N+1 媒体哈希值的哈希值 (Media Hash N. Hash) 和第 N+1 声明的哈希值 (Claim Hash N1) 封装在一起。例如, 可以将第二媒体哈希值的哈希值和第二声明的哈希值封装在一起, 在此不一一例举。示例性地, Trust Manifest 可以有多个, 第二声明可以有一个或多个, 例如, Trust Manifest

的个数与 Trust Record 类似, 在此不再赘述。

示例性地, 在图 8d 中, 第二媒体内容的元数据还可以包括第 N+1 统一资源定位符 (URL, Uniform Resource Locator), 第 N+1URL 指示第 N+1 声明或第 N+1 媒体哈希值在第 N+1 的元数据中的位置。例如, URL4 是第二媒体哈希值在第二媒体内容的元数据中的位置, URL5 是第 N+1 声明在第二媒体内容的元数据中的位置, URLi 是第 N+1 媒体哈希值在第 N+1 媒体内容的元数据中的位置, URLi+1 是第 N+1 声明在第 N+1 媒体内容的元数据中的位置, i 视具体环境而定, i 为正整数。

示例性地, 可以将第 N+1 媒体哈希值的哈希值、第 N+1 声明的哈希值和对应的 URL 封装在一起。

示例性地, 第 N+1 媒体内容的元数据还可以包括其它信息, 其它信息可以是不用于证实第 N+1 媒体内容的真实性的信息。例如: 文件名、哈希算法的名称, 哈希算法用于计算得到上述实施例提到的哈希值。

示例性地, 第 N+1 组合哈希值可以是第 N+1 声明的哈希值、第 N+1 媒体哈希值的哈希值和第 N+1URL 组合后的数据的哈希值。示例性地, 第 N+1 组合哈希值可以是第 N+1 声明的哈希值、第 N+1 媒体哈希值的哈希值、第 N+1URL 和其它信息组合后的哈希值。以下对 Trust Profile 的验证过程进行说明。

图 9a 为示例性示出的验证过程示意图。在图 9a 的实施例, 对图 2a 或图 3a 实施例中第一媒体内容的 Trust Profile 进行验证。应该理解的是, 对第一媒体内容的 Trust Profile 进行验证的电子设备, 可以是第一电子设备, 也可以是其他电子设备, 本申请对此不作限制。

S901, 获取第一媒体内容的元数据; 其中, 元数据包括: 第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名; 第一媒体哈希值是第一媒体内容的哈希值, 第一组合哈希值是根据初始信息和第一媒体哈希值确定的。

示例性地, 当需要对第一媒体内容进行溯源或判断第一媒体内容的真实性时, 可以从第一媒体内容的元数据中, 获取第一媒体内容的 Trust Profile; 然后执行 S902。

示例性地, 当第一媒体内容的 Trust Profile 如图 3a 实施例所示时, 可以对第一媒体内容的 Trust Profile 进行解封装, 得到 Trust Declaration; 之后, 对 Trust Declaration 进行解封装, 得到第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名。

S902, 对第一媒体内容的元数据进行验证。

示例性地, S902 可以是对第一媒体内容的 Trust Profile 进行验证。

图 9b 为示例性示出的验证过程示意图。参照图 9b, 示例性地, S902 可以包括如下 S9021~S9026:

S9021, 对第一媒体内容进行哈希计算, 得到第一预测媒体哈希值。

示例性地, 可以采用哈希算法对第一媒体内容进行哈希计算, 得到第一预测媒体哈希值。应该理解的是, S9021 采用的哈希算法与图 3a 实施例中 S302 采用的哈希算法相同。

S9022, 判断第一预测媒体哈希值与第一媒体内容的 Trust Profile 中第一媒体哈希值是否相同。

示例性地, 当第一预测媒体哈希值与第一媒体内容的 Trust Profile 中第一媒体哈希值相同时, 说明 Trust Profile 是第一媒体内容的 Trust Profile, 或者, 说明第一媒体哈希值没有被篡改, 此时可以执行 S9023, 继续对第一媒体内容的 Trust Profile 中的其他信息进行验证。当第一预测媒体哈希值与第一媒体内容的 Trust Profile 中第一媒体哈希值不相同, 说明 Trust Profile 不是第一媒体内容的 Trust Profile, 或者, 说明第一媒体哈希值被篡改; 此时, 可以确定对第一媒体内容的 Trust Profile 的验证失败。

S9023, 当第一媒体预测哈希值与第一 Trust Profile 中的第一媒体哈希值相同时, 根据第一媒体内容的初始信息和第一预测媒体哈希, 确定第一预测组合哈希值。

示例性地, 当第一媒体预测哈希值与第一媒体内容的 Trust Profile 中第一媒体哈希值相同时, 可以将第一媒体内容的初始信息和第一预测媒体哈希值进行组合 (也可以叫做连接或级联); 采用哈希算法对第一媒体内容的初始信息和第一预测媒体哈希值的组合进行哈希计算, 得到第一预测组合哈希值。

应该理解的是, S9023 采用的哈希算法与图 3a 实施例中 S303 采用的哈希算法相同。

S9024, 判断第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值是否相同。

示例性地, 当第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值相同时, 说明第一媒体内容的 Trust Profile 中的第一组合哈希值未被篡改, 以及第一媒体内容的初始信息未被篡改, 可以执行 S9025, 继续对第一媒体内容的 Trust Profile 中的其他信息进行验证。当第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值不相同, 说明第一媒体内容的 Trust Profile 中的第一组合哈希值被篡改或第一媒体内容的初始信息被篡改, 此时, 可以确定对第一媒体内容的 Trust Profile 的验证失

败。

S9025, 当第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值相同时, 根据第一公钥、第一组合哈希值和第一预测组合哈希值的数字签名进行第一签名验证。

示例性地, 第一公钥与第一私钥是一组密钥对。应该理解的是, S9025 在第一签名验证过程中涉及的数字签名算法, 与上述 S304 涉及的数字签名算法相同。

S9026, 判断第一签名验证是否成功。

示例性地, 当第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值相同时, 可以采用第一公钥对第一组合哈希值的数字签名进行解密, 得到解密哈希值; 判断解密哈希值与第一预测组合哈希值是否相同。

当解密哈希值与第一预测组合哈希值不相同, 说明第一签名验证失败, 此时, 可以确定对第一媒体内容的 Trust Profile 的验证失败, 即第一媒体内容的 Trust Profile 为假。

当解密哈希值与第一预测组合哈希值相同时, 说明第一签名验证成功, 此时, 可以对第一媒体内容的 Trust Profile 的验证成功, 即第一媒体内容的 Trust Profile 为真。示例性地, 当第一媒体内容的 Trust Profile 为真时, 用户可以进一步对第一媒体内容的真实性进行判断, 或者, 确定第一媒体内容中的内容为真, 本申请对此不作限制。

图 10a 为示例性示出的验证过程示意图。在图 10a 的实施例中, 对图 6a 或图 8a 实施例中第 N+1 媒体内容的 Trust Profile 进行验证。应该理解的是, 对第 N+1 媒体内容的 Trust Profile 进行验证的电子设备, 可以是第 N+1 电子设备, 也可以是其他电子设备, 本申请对此不作限制。

S1001, 获取第 N+1 媒体内容的元数据, 第 N+1 媒体内容的元数据包括第一媒体内容的初始信息、N+1 个媒体哈希值、N+1 个组合哈希值、N+1 个组合哈希值的数字签名、一个或多个第 N+1 媒体声明和一个或多个第 N+1 声明哈希值。

示例性地, 当需要对第 N+1 媒体内容进行溯源或判断第 N+1 媒体内容的真实性时, 可以从第 N+1 媒体内容的元数据中, 获取第 N+1 媒体内容的 Trust Profile; 然后执行 S1002。

示例性地, 当获取的第 N+1 媒体内容的 Trust Profile 为图 8a 生成的第 N+1 媒体内容的 Trust Profile 时, 可以对第 N+1 媒体内容的 Trust Profile 进行解封装, 得到 Trust Declaration、Trust Record 1、.....、Trust Record N; 之后, 可以对 Trust Declaration 和 Trust Record 1、.....、Trust Record N 分别解封装, 得到第一媒体内容的初始信息、N+1 个媒体哈希值、N+1 个组合哈希值、N+1 个组合哈希值的数字签名、一个或多个第 N+1 媒体声明和一个或多个第 N+1 声明哈希值。

S1002, 对第 N+1 媒体内容的元数据进行验证。

示例性地, S1002 可以是对第 N+1 媒体内容的 Trust Profile 进行验证。

图 10b 和图 10c 为示例性示出的验证过程示意图。参照图 10b 和图 10c, S1002 可以包括如下 S10021~S100224: 在图 10b 和 10c 的实施例中, 对图 6a 或图 8a 实施例中第 N+1 媒体内容的 Trust Profile 进行验证。

S10021, 根据第一媒体内容的初始信息和第一媒体哈希, 确定第一预测组合哈希值。

S10022, 判断第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值是否相同。

示例性地, 当第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值相同时, 可以执行 S10023。当第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值不相同, 可以确定对第 N+1 媒体内容的 Trust Profile 的验证失败。

S10023, 当第一预测组合哈希值与第一媒体内容的 Trust Profile 中的第一组合哈希值相同时, 根据第一公钥、第一组合哈希值和第一预测组合哈希值的数字签名进行第一签名验证。

示例性地, S10021~S10023 可以参照上述 S9023~S9025 的描述, 在此不再赘述。

S10024, 判断第一签名验证是否成功。

示例性地, 当第一签名验证成功时, 执行 S10025; 当第一签名验证失败时, 可以确定对第 N+1 媒体内容的 Trust Profile 的验证失败。

S10025, 当第一签名验证成功时, 对第 i 媒体声明进行哈希计算, 得到第 i 预测声明哈希值, i 的初始值为 2, i 为小于 N 的整数。

示例性地, 可以采用哈希算法对第 i 媒体声明进行哈希计算, 得到第 i 预测声明哈希值。应该理解的是, S10025 采用的哈希算法与 S602 采用的哈希算法相同。

示例性地, 当第  $i$  媒体声明包括多个时, 可以分别对每个第  $i$  媒体声明进行哈希计算, 得到每个第  $i$  媒体声明对应的第  $i$  预测声明哈希值。

S10026, 判断第  $i$  预测声明哈希值和第  $N+1$  媒体内容的 Trust Profile 中的第  $i$  声明哈希值是否相同。

5 示例性地, 当第  $i$  媒体声明包括多个时, 可以依次判断每个第  $i$  媒体声明对应的第  $i$  预测声明哈希值与第  $i$  声明哈希值是否相同。当所有第  $i$  媒体声明对应的第  $i$  预测声明哈希值与第  $i$  声明哈希值均相同时, 可以执行 S10027。当至少一个第  $i$  媒体声明对应的第  $i$  预测声明哈希值与第  $i$  声明哈希值不相同, 可以确定对第  $N+1$  媒体内容的 Trust Profile 验证失败。

S10027, 当第  $i$  预测声明哈希值和第  $N+1$  媒体内容的 Trust Profile 中的第  $i$  声明哈希值时, 判断  $i$  是否小于  $N-1$ 。

10 示例性地, 若  $i$  小于  $N-1$ , 则执行 S10028; 若  $k$  等于  $N-1$ , 则执行 S10029。

S10028, 将  $i$  加 1, 并返回执行 S10025。

应该理解的是, S10025~S10028 是可选步骤, 具体根据第  $N+1$  媒体内容的 Trust Profile 中是否包括第  $i$  媒体声明和第  $i$  声明哈希值。

15 S10029, 根据第  $k$  组合哈希值、第  $k+1$  媒体哈希值和第  $k+1$  组声明哈希值, 确定第  $k+1$  预测组合哈希值,  $k$  的初始值为 1,  $k$  为小于  $N$  的整数。

S100210, 判断第  $k+1$  预测组合哈希值与第  $N+1$  媒体内容的 Trust Profile 中的第  $k+1$  组合哈希值是否相同。

20 示例性地, 当第  $k+1$  预测组合哈希值与第  $N+1$  媒体内容的 Trust Profile 中的第  $k+1$  组合哈希值相同时, 可以执行 S100211; 当第  $k+1$  预测组合哈希值与第  $N+1$  媒体内容的 Trust Profile 中的第  $k+1$  组合哈希值不相同, 可以确定对第  $N+1$  媒体内容的 Trust Profile 验证失败。

S100211, 当第  $k+1$  预测组合哈希值与第  $N+1$  媒体内容的 Trust Profile 中的第  $k+1$  组合哈希值相同时, 判断  $k$  是否小于  $N-2$ 。

示例性地, 若  $k$  小于  $N-1$ , 则执行 S100212; 若  $k$  等于  $N-1$ , 则执行 S100213。

S100212, 将  $k$  加 1, 并返回执行 S10029。

25 S100213, 根据第  $j$  公钥、第  $j$  组合哈希值和第  $j$  组合哈希值的数字签名进行第  $j$  签名验证,  $j$  的初始值为 1,  $j$  为小于  $N$  的整数。

示例性地, 第  $j$  公钥与第  $j$  私钥是一组密钥对。应该理解的是, S100213 在第  $j$  签名验证过程中涉及的数字签名算法, 与 Trust Profile 生成过程中采用第  $j$  私钥进行数字签名所涉及的数字签名算法相同。

S100214, 判断第  $j$  签名验证是否成功。

30 示例性地, 若第  $j$  签名验证成功, 则执行 S100215; 若第  $j$  签名验证识别, 则说明对第  $N+1$  媒体内容的 Trust Profile 验证失败。

S100215, 判断  $j$  是否小于  $N$ 。

示例性地, 若  $j$  小于  $N$ , 则执行 S100216; 若  $j$  等于  $N$ , 则执行 S100217。

S100216, 将  $j$  加 1, 并返回执行 S100213。

35 应该理解的是, S10029~S100216 是可选步骤, 具体根据第  $N+1$  媒体内容的 Trust Profile 中是否包括第  $k$  组合哈希值和第  $k$  组合哈希值的数字签名。

S100217, 对第  $N+1$  媒体内容进行哈希计算, 得到第  $N+1$  预测媒体哈希值。

S100218, 判断第  $N+1$  预测媒体哈希值与第  $N+1$  媒体内容的 Trust Profile 中第  $N+1$  媒体哈希值是否相同。

40 示例性地, 当第  $N+1$  预测媒体哈希值与第  $N+1$  媒体内容的 Trust Profile 中第  $N+1$  媒体哈希值相同时, 则执行 S100219。当第  $N+1$  预测媒体哈希值与第  $N+1$  媒体内容的 Trust Profile 中第  $N+1$  媒体哈希值不相同, 则说明对第  $N+1$  媒体内容的 Trust Profile 验证失败。

S100219, 当第  $N+1$  预测媒体哈希值与第  $N+1$  媒体内容的 Trust Profile 中第  $N+1$  媒体哈希值相同时, 对第  $N+1$  声明进行哈希计算, 得到第  $N+1$  预测声明哈希值。

45 S100220, 判断第  $N+1$  预测声明哈希值和第  $N+1$  媒体内容的 Trust Profile 中的第  $N+1$  声明哈希值是否相同。

示例性地, 当第  $N+1$  预测声明哈希值和第  $N+1$  媒体内容的 Trust Profile 中的第  $N+1$  声明哈希值相同时, 则执行 S100221。当第  $N+1$  预测声明哈希值和第  $N+1$  媒体内容的 Trust Profile 中的第  $N+1$  声明哈希值

不相同，则说明对第 N+1 媒体内容的 Trust Profile 验证失败。

应该理解的是，S100219~S100220 是可选步骤，具体根据第 N+1 媒体内容的 Trust Profile 中是否包括第 N+1 媒体声明和第 N+1 声明哈希值。

5 S100221，当第 N+1 预测声明哈希值和第 N+1 媒体内容的 Trust Profile 中的第 N+1 声明哈希值相同时，根据第 N 组合哈希值、第 N+1 预测声明哈希值和第 N+1 预测声明哈希值，确定第 N+1 预测组合哈希值。

S100222，判断第 N+1 预测组合哈希值和第 N+1 媒体内容的 Trust Profile 中的第 N+1 组合哈希值是否相同。

10 示例性地，当第 N+1 预测组合哈希值和第 N+1 媒体内容的 Trust Profile 中的第 N+1 组合哈希值相同时，则执行 S100223。当第 N+1 预测组合哈希值和第 N+1 媒体内容的 Trust Profile 中的第 N+1 组合哈希值不相同，则说明对第 N+1 媒体内容的 Trust Profile 验证失败。

S100223，当第 N+1 预测组合哈希值和第 N+1 媒体内容的 Trust Profile 中的第 N+1 组合哈希值时，根据第 N+1 公钥、第 N+1 预测组合哈希值和第 N+1 组合哈希值的数字签名进行第 N+1 签名验证。

15 示例性地，第 N+1 公钥与第 N+1 私钥是一组密钥对。应该理解的是，S100223 在第 N+1 签名验证过程中涉及的数字签名算法，与 Trust Profile 生成过程中采用第 N+1 私钥进行数字签名所涉及的数字签名算法相同。

S100224，判断第 N+1 签名验证是否成功。

20 示例性地，当第 N+1 签名验证失败，此时，可以确定对第 N+1 媒体内容的 Trust Profile 的验证失败。当第 N+1 签名验证成功，此时，可以确定对第 N+1 媒体内容的 Trust Profile 的验证成功。示例性地，当 Trust Profile 为真时，用户可以进一步对第 N+1 媒体内容的真实性进行判断，或者，认为第 N+1 媒体内容中的内容为真，本申请对此不作限制。

应该理解的是，S100221~S100224 是可选步骤，具体根据第 N+1 媒体内容的 Trust Profile 中是否包括第 N+1 组合哈希值和第 N+1 组合哈希值的数字签名。

在图 10d 和 10e 的实施例中，对图 6b 或图 8b 实施例中第 N+1 媒体内容的 Trust Profile 进行验证。

25 图 10d 和 10e 中的验证方法与图 10b 和 10c 的验证方法的区别在于 S10023 和 S100221 步骤，S10023 步骤的区别是根据第 k 组合哈希值、第 k 组合哈希值的数字签名、第 k+1 媒体哈希值和第 k+1 组声明哈希值，确定第 k+1 预测组合哈希值，k 的初始值为 1，k 为小于 N 的整数；S100221 步骤的区别是根据第 N 组合哈希值、第 N 组合哈希值的数字签名、第 N+1 预测声明哈希值和第 N+1 预测声明哈希值，确定第 N+1 预测组合哈希值。

30 图 11 为示例性示出的元数据的生成装置示意图。该元数据的生成装置可以用于执行前述实施例的方法，因此，其所能达到的有益效果可参考上文所提供的对应的方法中的有益效果，此处不再赘述。

参照图 11，示例性地，元数据的生成装置可以包括：

第一数据获取模块 1101，用于获取第一媒体内容；

35 第一信息生成模块 1102，用于生成第一媒体内容的元数据，第一媒体内容的元数据包括：第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名；第一媒体哈希值是第一媒体内容的哈希值，第一组合哈希值是初始信息和第一媒体哈希值的组合的哈希值。

示例性地，元数据的生成装置还可以包括：

第一哈希计算模块，用于对第一媒体内容进行哈希计算，得到第一媒体哈希值。

40 示例性地，第一哈希计算模块，还用于根据初始信息和第一媒体哈希值的组合进行哈希计算，得到第一组合哈希值。

示例性地，元数据的生成装置还可以包括：

第一封装模块，用于根据第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名，得到信任声明。

45 图 12 为示例性示出的元数据的生成装置示意图。该元数据的生成装置可以用于执行前述实施例的方法，因此，其所能达到的有益效果可参考上文所提供的对应的方法中的有益效果，此处不再赘述。

参照图 12，示例性地，元数据的生成装置可以包括：

第二数据获取模块 1201，获取第 N+1 媒体内容，第 N+1 媒体内容基于第 N 媒体内容得到；

第二信息生成模块 1202，用于生成第 N+1 媒体内容的元数据，第 N+1 媒体内容的元数据包括第一媒

体内容的初始信息、第一组合哈希值和第一组合哈希值的数字签名，第一组合哈希值是初始信息和第一媒体哈希值的组合的哈希值；N+1 媒体内容的元数据还包括 N+1 个媒体哈希值，其中，第 N+1 媒体哈希值是第 N+1 媒体内容的哈希值，第一媒体哈希值是第一媒体内容的哈希值；N 为正整数。

示例性地，元数据的生成装置还可以包括：

- 5 第二哈希计算模块，用于将第 N 组合哈希值、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中的一个或多个哈希值连接后进行哈希计算，得到中间哈希值；其中，中间哈希值用于确定第 N+1 组合哈希值。

示例性地，第二哈希计算模块，还用于将第 N 组合哈希值、第 N 组合哈希值的数字签名、一个或多个第 N+1 声明哈希值和第 N+1 媒体哈希值中的一个或多个哈希值连接后进行哈希计算，得到中间哈希值。

- 10 示例性地，第二哈希计算模块，还用于基于中间哈希值，确定第 N+1 组合哈希值。

示例性地，第二哈希计算模块，还用于对第 N+1 媒体内容进行哈希计算，得到第 N+1 媒体哈希值。

示例性地，元数据的生成装置还可以包括：

第二封装模块，用于根据初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名，得到信任声明。

- 15 示例性地，第二封装模块，还用于根据第 N+1 媒体哈希值、第 N+1 组合哈希值和第 N+1 组合哈希值的数字签名，得到信任记录。

示例性地，第二封装模块，还用于根据信任声明和信任记录，得到第 N+1 媒体内容的信任档案。

- 需要说明的是，当图 11 实施例中的元数据的生成装置与图 12 实施例中的元数据的生成装置属于同一电子设备时，则图 11 实施例中的元数据的生成装置与图 12 实施例中的元数据的生成装置为同一装置；此时，第一数据获取模块 1101 与第二数据获取模块 1201 为同一模块，第一信息生成模块 1102 和第二信息生成模块 1202 为同一模块，第一哈希计算模块和第二哈希计算模块为同一模块，以及第一封装模块和第二封装模块为同一模块。

- 20 当图 11 实施例中的元数据的生成装置与图 12 实施例中的元数据的生成装置属于不同的电子设备时，则图 11 实施例中的元数据的生成装置与图 12 实施例中的元数据的生成装置为不同的两个装置；此时，第一数据获取模块 1101 与第二数据获取模块 1201 是不同的两个模块，第一信息生成模块 1102 和第二信息生成模块 1202 是不同的两个模块，第一哈希计算模块和第二哈希计算模块是不同的两个模块，以及第一封装模块和第二封装模块是不同的两个模块。

图 13 为示例性示出的验证装置示意图。该验证装置可以用于执行前述实施例的方法，因此，其所能达到的有益效果可参考上文所提供的对应的方法中的有益效果，此处不再赘述。

- 30 参照图 13，示例性地，验证装置可以包括：

第一信息获取模块 1301，用于获取第一媒体内容的元数据；其中，元数据包括：第一媒体内容的初始信息、第一媒体哈希值、第一组合哈希值和第一组合哈希值的数字签名；第一媒体哈希值是第一媒体内容的哈希值，第一组合哈希值是初始信息和第一媒体哈希值的组合的哈希值；

第一验证模块 1302，用于对第一媒体内容的元数据进行验证。

- 35 图 14 为示例性示出的验证装置示意图。该验证装置可以用于执行前述实施例的方法，因此，其所能达到的有益效果可参考上文所提供的对应的方法中的有益效果，此处不再赘述。

参照图 14，示例性地，验证装置可以包括：

- 40 第二信息获取模块 1401，用于获取第 N+1 媒体内容的元数据；其中，第 N+1 媒体内容基于第 N 媒体内容得到，第 N+1 媒体内容的元数据包括第一媒体内容的初始信息、第一组合哈希值和第一组合哈希值的数字签名，第一组合哈希值是初始信息和第一媒体哈希值的组合的哈希值；N+1 媒体内容的元数据还包括 N+1 个媒体哈希值，其中，第 N+1 媒体哈希值是第 N+1 媒体内容的哈希值，第一媒体哈希值是第一媒体内容的哈希值；N 为正整数；

第二验证模块 1402，用于对第 N+1 媒体内容的元数据进行验证。

- 45 需要说明的是，当图 13 实施例中的验证装置与图 14 实施例中的验证装置属于同一电子设备时，则图 13 实施例中的验证装置与图 14 实施例中的验证装置为同一装置；此时，第一信息获取模块 1301 与第二信息获取模块 1401 为同一模块，以及第一验证模块 1302 和第二验证模块 1402 为同一模块。

当图 13 实施例中的验证装置与图 14 实施例中的验证装置属于不同的两个电子设备时，则图 13 实施例中的验证装置与图 14 实施例中的验证装置为不同的两个装置；此时，第一信息获取模块 1301 与第二信

息获取模块 1401 是不同的两个模块, 以及第一验证模块 1302 和第二验证模块 1402 是不同的两个模块。

一个示例中, 图 15 示出了本申请实施例的一种装置 1500 的示意性框图装置 1500 可包括: 处理器 1501 和收发器/收发管脚 1502, 可选地, 还包括存储器 1503。

5 装置 1500 的各个组件通过总线 1504 耦合在一起, 其中总线 1504 除包括数据总线之外, 还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见, 在图中将各种总线都称为总线 1504。

可选地, 存储器 1503 可以用于存储前述方法实施例中的指令。该处理器 1501 可用于执行存储器 1503 中的指令, 并控制接收管脚接收信号, 以及控制发送管脚发送信号。

装置 1500 可以是上述方法实施例中的电子设备或电子设备的芯片。

10 其中, 上述方法实施例涉及的所有相关内容均可以援引到对应功能模块的功能描述, 在此不再赘述。

本申请实施例还提供一种芯片, 包括一个或多个接口电路和一个或多个处理器; 一个或多个处理器通过一个或多个接口电路接收或发送数据, 当一个或多个处理器执行计算机指令时, 使得电子设备上述相关方法步骤实现上述实施例中的方法。其中, 接口电路为收发器/收发管脚 1502。

15 本实施例还提供一种计算机可读存储介质, 该计算机可读存储介质中存储有计算机指令, 当该计算机指令在电子设备上运行时, 使得电子设备执行上述相关方法步骤实现上述实施例中的方法。

本实施例还提供了一种计算机程序产品, 该计算机程序产品包含计算机指令, 当计算机指令被计算机或处理器执行时, 使得计算机执行上述相关步骤, 以实现上述实施例中的方法。

20 另外, 本申请的实施例还提供一种装置, 这个装置具体可以是芯片, 组件或模块, 该装置可包括相连的处理器和存储器; 其中, 存储器用于存储计算机执行指令, 当装置运行时, 处理器可执行存储器存储的计算机执行指令, 以使芯片执行上述各方法实施例中的方法。

其中, 本实施例提供的电子设备、计算机可读存储介质、计算机程序产品或芯片均用于执行上文所提供的对应的方法, 因此, 其所能达到的有益效果可参考上文所提供的对应的方法中的有益效果, 此处不再赘述。

25 通过以上实施方式的描述, 所属领域的技术人员可以了解到, 为描述的方便和简洁, 仅以上述各功能模块的划分进行举例说明, 实际应用中, 可以根据需要而将上述功能分配由不同的功能模块完成, 即将装置的内部结构划分成不同的功能模块, 以完成以上描述的全部或者部分功能。

在本申请所提供的几个实施例中, 应该理解到, 所揭露的装置和方法, 可以通过其它的方式实现。例如, 以上所描述的装置实施例仅仅是示意性的, 例如, 模块或单元的划分, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式, 例如多个单元或组件可以结合或者可以集成到另一个装置, 或一些特征可以忽略, 或不执行。另一点, 所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口, 装置或单元的间接耦合或通信连接, 可以是电性, 机械或其它的形式。

30 作为分离部件说明的单元可以是或者也可以不是物理上分开的, 作为单元显示的部件可以是一个物理单元或多个物理单元, 即可以位于一个地方, 或者也可以分布到多个不同地方。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

35 另外, 在本申请各个实施例中的各功能单元可以集成在一个处理单元中, 也可以是各个单元单独物理存在, 也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现, 也可以采用软件功能单元的形式实现。

本申请各个实施例的任意内容, 以及同一实施例的任意内容, 均可以自由组合。对上述内容的任意组合均在本申请的范围之内。

40 集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用, 可以存储在一个可读存储介质中。基于这样的理解, 本申请实施例的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来, 该软件产品存储在一个存储介质中, 包括若干指令用以使得一个设备(可以是单片机, 芯片等)或处理器(processor)执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括: U 盘、移动硬盘、只读存储器(read only memory, ROM)、随机存取存储器(random access memory, RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

45 上面结合附图对本申请的实施例进行了描述, 但是本申请并不局限于上述的具体实施方式, 上述的具体实施方式仅仅是示意性的, 而不是限制性的, 本领域的普通技术人员在本申请的启示下, 在不脱离本申请宗旨和权利要求所保护的范围情况下, 还可做出很多形式, 均属于本申请的保护之内。

结合本申请实施例公开内容所描述的方法或者算法的步骤可以硬件的方式来实现，也可以是由处理器执行软件指令的方式来实现。软件指令可以由相应的软件模块组成，软件模块可以被存放于随机存取存储器（Random Access Memory, RAM）、闪存、只读存储器（Read Only Memory, ROM）、可擦除可编程只读存储器（Erasable Programmable ROM, EPROM）、电可擦可编程只读存储器（Electrically EPROM, EEPROM）、寄存器、硬盘、移动硬盘、只读光盘（CD-ROM）或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于 ASIC 中。

本领域技术人员应该可以意识到，在上述一个或多个示例中，本申请实施例所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机可读存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

上面结合附图对本申请的实施例进行了描述，但是本申请并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本申请的启示下，在不脱离本申请宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本申请的保护之内。

权 利 要 求 书

1. 一种元数据的生成方法，其特征在于，所述方法包括：  
获取第一媒体内容；  
生成所述第一媒体内容的元数据，所述第一媒体内容的元数据包括：所述第一媒体内容的初始信息、  
5 第一媒体哈希值和第一数字签名；所述第一媒体哈希值是所述第一媒体内容的哈希值，所述第一数字签名  
是第一数据的数字签名，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据。
2. 根据权利要求1所述的方法，其特征在于，所述第一数据是至少由所述第一媒体哈希值和所述第一  
10 媒体内容的初始信息组合后的数据，或者，所述第一数据是至少由所述初始信息的哈希值和所述第一媒体  
哈希值的哈希值组合后的数据。
3. 根据权利要求1所述的方法，其特征在于，所述第一数据是至少根据所述初始信息和所述第一媒体  
哈希值确定的哈希值。
- 15 4. 根据权利要求3所述的方法，其特征在于，所述第一数据是至少由所述第一媒体哈希值的哈希值和  
所述第一媒体内容的初始信息的哈希值确定的哈希值，或者，所述第一数据是至少由所述初始信息和所述  
第一媒体哈希值组合后的数据的哈希值。
- 20 5. 根据权利要求1至4任一项所述的方法，其特征在于，所述第一媒体内容的元数据还包括所述第一  
数据。
6. 根据权利要求1所述的方法，其特征在于，所述第一媒体内容的元数据还包括所述第一媒体哈希值  
的哈希值和所述第一媒体内容的初始信息的哈希值。
- 25 7. 根据权利要求6所述的方法，其特征在于，所述第一媒体内容的元数据还包括：第一统一资源定位  
符（URL），所述第一 URL 指示所述第一媒体内容的初始信息或所述第一媒体哈希值在所述第一媒体内  
容的元数据中的位置。
- 30 8. 根据权利要求6所述的方法，其特征在于，所述第一数据是至少由所述第一媒体哈希值的哈希值、  
所述第一媒体内容的初始信息的哈希值和所述统一资源定位符组合后的数据的哈希值。
9. 根据权利要求6至8任一项所述的方法，其特征在于，所述生成所述第一媒体内容的元数据包括：  
获取所述第一媒体内容的初始信息和所述第一媒体哈希值；  
至少封装所述第一媒体内容的初始信息、所述第一媒体哈希值，得到第一封装数据（Trust Indicators）；  
35 对所述第一媒体哈希值进行哈希计算，得到所述第一媒体哈希值的哈希值；对所述第一媒体内容的初  
始信息进行哈希计算，得到所述第一媒体内容的初始信息的哈希值；  
至少封装所述第一媒体哈希值的哈希值和所述第一媒体内容的初始信息的哈希值，得到第二封装数据  
（Declaration Hash）；  
对所述第一数据进行数字签名，所述第一数据是至少由所述第一媒体哈希值的哈希值和所述第一媒体  
40 内容的初始信息的哈希值确定的数据，得到所述第一数字签名；  
至少封装所述第一封装数据、所述第二封装数据和所述第一数字签名，得到信任声明；  
至少根据所述信任声明得到所述第一媒体内容的元数据。
10. 根据权利要求1所述的方法，其特征在于，所述生成所述第一媒体内容的元数据包括：  
45 获取所述第一媒体内容的初始信息和所述第一媒体哈希值；  
至少封装所述第一媒体内容的初始信息、所述第一媒体哈希值，得到第一封装数据（Trust Indicators）；  
对所述第一数据进行数字签名，得到所述第一数字签名，所述第一数据是至少由所述第一媒体哈希值

和所述第一媒体内容的初始信息确定的数据；

至少封装所述信任指标和所述第一组合哈希值的数字签名，得到信任声明；

至少根据所述信任声明得到所述第一媒体内容的元数据。

5 11. 根据权利要求 1 至 10 任一项所述的方法，其特征在于，

所述第一媒体内容的初始信息包括以下至少一种：所述第一媒体内容的生成时间、所述第一媒体内容的作者名称、所述第一媒体内容的数字内容标识、所述第一媒体内容的生成地点、所述第一媒体内容的生成设备的信息、所述第一媒体内容的分辨率、所述第一媒体内容的大小、所述第一媒体内容的媒体类型、所述第一媒体内容的版权信息或所述第一媒体内容的生成方式。

10

12. 一种元数据的生成方法，其特征在于，所述方法包括：

获取第 N+1 媒体内容，所述第 N+1 媒体内容基于第 N 媒体内容得到；

生成所述第 N+1 媒体内容的元数据，所述第 N+1 媒体内容的元数据包括第一媒体内容的初始信息和第一数据的数字签名；所述 N+1 媒体内容的元数据还包括 N 个媒体哈希值，其中，第一媒体哈希值是所述第一媒体内容的哈希值，第 N+1 媒体哈希值是所述第 N+1 媒体内容的哈希值，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据；N 为正整数。

15

13. 根据权利要求 12 所述的方法，其特征在于，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的哈希值。

20

14. 根据权利要求 13 所述的方法，其特征在于，所述第一数据是至少由所述第一媒体哈希值的哈希值和所述第一媒体内容的初始信息的哈希值确定的哈希值，或者，所述第一数据是至少由所述初始信息和所述第一媒体哈希值组合后的数据的哈希值。

25

15. 根据权利要求 12 至 14 任一项所述的方法，其特征在于，所述第一媒体内容的元数据还包括所述第一数据。

16. 根据权利要求 12 所述的方法，其特征在于，所述第一媒体内容的元数据还包括所述第一媒体哈希值的哈希值和所述第一媒体内容的初始信息的哈希值。

30

17. 根据权利要求 16 所述的方法，其特征在于，所述第一媒体内容的元数据还包括：第一统一资源定位符（URL），所述第一 URL 指示所述第一媒体内容的初始信息或所述第一媒体哈希值在所述第一媒体内容的元数据中的位置。

35

18. 根据权利要求 17 所述的方法，其特征在于，所述第一数据是至少由所述第一媒体哈希值的哈希值、所述第一媒体内容的初始信息的哈希值和所述统一资源定位符组合后的数据的哈希值。

19. 根据权利要求 12 所述的方法，其特征在于，所述第 N+1 媒体内容的元数据还包括第 N+1 声明。

40

20. 根据权利要求 19 所述的方法，其特征在于，所述第 N+1 媒体内容的元数据还包括第 N+1 媒体哈希值的哈希值和第 N+1 声明的哈希值。

21. 根据权利要求 19 所述的方法，其特征在于，所述第 N+1 媒体内容的元数据还包括 N 个数字签名，所述第 N+1 数字签名是第 N+1 数据的数字签名，所述第 N+1 数据是基于至少根据所述 N+1 声明和所述第 N+1 媒体哈希值确定的数据。

45

22. 根据权利要求 21 所述的方法，其特征在于，所述第 N+1 数据是至少根据所述 N+1 声明和所述第 N+1 媒体哈希值确定的哈希值。

23. 根据权利要求 22 所述的方法，其特征在于，所述第 N+1 数据是至少由所述 N+1 声明的哈希值和所述第 N+1 媒体哈希值的哈希值确定的哈希值，或者，所述第 N+1 数据是至少由所述第 N+1 声明和所述第 N+1 媒体哈希值组合后的数据的哈希值。
- 5
24. 根据权利要求 12 所述的方法，其特征在于，所述第 N+1 媒体内容的元数据还包括第 N+1 统一资源定位符（URL），所述第 N+1 URL 指示所述第 N+1 声明和所述第 N+1 媒体哈希值在所述第 N+1 媒体内容的元数据中的位置。
- 10
25. 根据权利要求 24 所述的方法，其特征在于，所述第 N+1 数据是至少由所述第 N+1 声明的哈希值、所述第 N+1 媒体哈希值的哈希值和所述第 N+1 URL 组合后的数据的哈希值。
- 15
26. 根据权利要求 21 所述的方法，其特征在于，所述第 N+1 媒体内容的元数据还包括第 N+1 数据，所述第 N+1 数据是基于至少根据所述 N+1 声明和所述第 N+1 媒体哈希值确定的数据。
27. 一种验证方法，其特征在于，所述方法包括：  
获取第一媒体内容的元数据；其中，所述元数据包括：所述第一媒体内容的初始信息、第一媒体哈希值和第一数字签名；所述第一媒体哈希值是所述第一媒体内容的哈希值，所述第一数字签名是第一数据的数字签名，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据；  
20 对所述第一媒体内容的元数据进行验证。
28. 一种验证方法，其特征在于，所述方法包括：  
获取第 N+1 媒体内容的元数据；其中，所述第 N+1 媒体内容的元数据包括第一媒体内容的初始信息和第一数据的数字签名；所述 N+1 媒体内容的元数据还包括 N 个媒体哈希值，其中，第 N+1 媒体哈希值是所述第 N+1 媒体内容的哈希值，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据；N 为正整数；  
25 对所述第 N+1 媒体内容的元数据进行验证。
29. 一种元数据的生成装置，其特征在于，所述装置包括：  
30 第一数据获取模块，用于获取第一媒体内容；  
第一信息生成模块，用于生成所述第一媒体内容的元数据，所述第一媒体内容的元数据包括：所述第一媒体内容的初始信息、第一媒体哈希值和第一数字签名；所述第一媒体哈希值是所述第一媒体内容的哈希值，所述第一数字签名是第一数据的数字签名，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据。
- 35
30. 一种元数据的生成装置，其特征在于，所述装置包括：  
第二数据获取模块，获取第 N+1 媒体内容，所述第 N+1 媒体内容基于第 N 媒体内容得到；  
第二信息生成模块，用于生成所述第 N+1 媒体内容的元数据，所述第 N+1 媒体内容的元数据包括第一媒体内容的初始信息和第一数据的数字签名；所述 N+1 媒体内容的元数据还包括 N 个媒体哈希值，其中，第 N+1 媒体哈希值是所述第 N+1 媒体内容的哈希值，所述第一数据是至少根据所述初始信息和所述  
40 第一媒体哈希值确定的数据；N 为正整数。
31. 一种验证装置，其特征在于，所述装置包括：  
第一信息获取模块，用于获取第一媒体内容的元数据；其中，所述元数据包括：所述第一媒体内容的  
45 初始信息、第一媒体哈希值和第一数字签名；所述第一媒体哈希值是所述第一媒体内容的哈希值，所述第一数字签名是第一数据的数字签名，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据；  
第一验证模块，用于对所述第一媒体内容的元数据进行验证。

32. 一种验证装置，其特征在于，所述装置包括：  
第二信息获取模块，用于获取第 N+1 媒体内容的元数据；其中，所述第 N+1 媒体内容的元数据包括第一媒体内容的初始信息和第一数据的数字签名；所述 N+1 媒体内容的元数据还包括 N 个媒体哈希值，  
5 其中，第 N+1 媒体哈希值是所述第 N+1 媒体内容的哈希值，所述第一数据是至少根据所述初始信息和所述第一媒体哈希值确定的数据；N 为正整数；  
第二验证模块，用于对所述第 N+1 媒体内容的元数据进行验证。
33. 一种电子设备，其特征在于，包括：  
10 存储器和处理器，所述存储器与所述处理器耦合；  
所述存储器存储有程序指令，当所述程序指令由所述处理器执行时，使得所述电子设备执行如权利要求 1 至权利要求 11 中任一项所述的方法。
34. 一种电子设备，其特征在于，包括：  
15 存储器和处理器，所述存储器与所述处理器耦合；  
所述存储器存储有程序指令，当所述程序指令由所述处理器执行时，使得所述电子设备执行如权利要求 12 至权利要求 26 中任一项所述的方法。
35. 一种电子设备，其特征在于，包括：  
20 存储器和处理器，所述存储器与所述处理器耦合；  
所述存储器存储有程序指令，当所述程序指令由所述处理器执行时，使得所述电子设备执行如权利要求 27 或权利要求 28 所述的方法。
36. 一种芯片，其特征在于，包括一个或多个接口电路和一个或多个处理器；所述一个或多个处理器  
25 通过所述一个或多个接口电路接收或发送数据，当所述一个或多个处理器执行计算机指令时，使得电子设备执行如权利要求 1 至权利要求 26 中任一项所述的方法。
37. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机程序，当所述计算机程序运行在计算机或处理器上时，使得所述计算机或所述处理器执行如权利要求 1 至权利要求 26 任  
30 一项所述的方法。
38. 一种计算机程序产品，其特征在于，所述计算机程序产品包含计算机指令，当所述计算机指令被计算机或处理器执行时，使得如权利要求 1 至权利要求 26 任一项所述的方法的步骤被执行。