

## 用户的身份内容信息的认证、验证方法和装置

### 技术领域

[01]本说明书涉及网络通信技术领域，尤其涉及用户的身份内容信息的认证、验证方法和装置。

### 5 背景技术

[02]CA 认证机构在生成数字证书时，通常将用户的全部身份信息，包括名称、身份号码（机构用户为社会统一信用代码或机构验证码，个人用户为身份证号码）、地址等，以明文的格式、或可被反向解码的编码格式（如 base 64）保存在数字证书中，在上述数字证书被验证时，上述数字证书内包含的全部身份信息均可被验证机构获得，而对上述全部身份信息的披露多数情况下是不必要的。现在仍缺少一种经 CA 认证机构认证的、可选择性地披露用户的身份信息的数字证书。

### 发明内容

- [03]针对以上提出的问题，本说明书提供了一种用户的身份内容信息的认证方法，包括：
- [04]获取用户的多个身份内容信息；
- 15 [05]基于所述用户的多个身份内容信息构建默克尔树，所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的；
- [06]向存储终端发送所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值。
- 20 [07]更优地，所述默克尔树的叶节点是基于用户的身份内容信息与其他数据信息而编码生成的；
- [08]所述方法还包括：向所述存储终端发送所述其他数据信息与所述叶节点的对应关系。
- [09]更优地，所述其他数据信息为随机数。
- [10]更优地，所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数

数据库中的一个或多个。

[11]更优地，所述存储终端包括认证机构的服务器；

[12]所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中；

5 [13]其中，所述数字证书包括内容部分与签名部分，所述内容部分包括基于用户的多个身份内容信息构建的默克尔树的根值，所述签名部分是对所述内容部分的电子签名。

[14]更优地，所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。

10 [15]更优地，所述存储终端还包括用户的客户端或区块链的分布式数据库，所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。

[16]更优地，所述用户的数字证书的内容部分还包括所述用户的公钥。

15 [17]更优地，所述用户的身份内容信息包括用户的公钥、用户的名称、用户的地址、用户的识别号码中的一种或多种。

[18]更优地，所述编码包括哈希编码。

[19]本说明书还提供了一种用户的身份内容信息的验证方法，包括：

20 [20]响应于待验证的身份内容信息，根据所述待验证的身份内容信息与基于用户的多个身份内容信息构建的默克尔树的叶节点的对应关系，从存储终端获取所述待验证的身份内容信息对应的叶节点的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值，其中，所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的；

[21]基于所述待验证的身份内容信息和所述默克尔证明，计算所述待验证的身份内容信息对应的默克尔树的根值；

25 [22]确定所述待验证的身份内容信息对应的默克尔树的根值与所述基于用户的多个身份内容信息构建的默克尔树的根值是否相同。

[23]更优地，所述默克尔树的叶节点是基于用户的身份内容信息与其他数据信息而编码生成的；

- [24]所述方法还包括:从所述存储终端获取所述其他数据信息与所述叶节点的对应关系;
- [25]所述基于所述待验证的身份内容信息和所述默克尔证明,计算所述待验证的身份内容信息对应的默克尔树的根值,包括:
- [26]基于所述待验证的身份内容信息、所述其他数据信息和所述默克尔证明,计算所述待验证的身份内容信息对应的默克尔树的根值。
- 5 [27]更优地,所述其他数据信息为随机数。
- [28]更优地,所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。
- [29]更优地,所述存储终端包括认证机构的服务器;
- 10 [30]所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中,其中,所述数字证书包括内容部分与签名部分,所述内容部分包括基于用户的多个身份内容信息构建的默克尔树的根值,所述签名部分是对所述内容部分的电子签名;
- [31]所述从存储终端获取所述基于用户的多个身份内容信息构建的默克尔树的根值,包括:
- 15 [32]获取所述用户的数字证书;
- [33]利用所述数字证书的认证机构对应的公钥验签所述数字证书;
- [34]在所述验签通过后,获取所述基于用户的多个身份内容信息构建的默克尔树的根值。
- [35]更优地,所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明;
- 20 [36]所述从存储终端获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明,包括:
- [37]获取所述用户的数字证书;
- 25 [38]利用所述数字证书的认证机构对应的公钥验签所述数字证书;
- [39]在所述验签通过后,获取待验证的身份内容信息与所述叶节点的对应关系,根据所述待验证的身份内容信息与所述叶节点的对应关系,获取所述待验证的身份内容信息对

应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。

[40]更优地，所述存储终端还包括用户的客户端或区块链的分布式数据库，所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户5 的客户端或所述区块链的分布式数据库。

[41]更优地，所述用户的数字证书的内容部分还包括所述用户的公钥。

[42]更优地，所述用户的身份内容信息包括用户的公钥、用户的名称、用户的地址、用户的识别号码中的一种或多种。

[43]更优地，所述编码包括哈希编码。

10 [44]本说明书还提供了一种用户的身份内容信息的认证装置，包括：

[45]获取单元，获取用户的多个身份内容信息；

[46]默克尔树构建单元，基于所述用户的多个身份内容信息构建默克尔树，所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的；

[47]发送单元，向存储终端发送所述用户的多个身份内容信息与所述叶节点的对应关系、15 所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值。

[48]更优地，所述默克尔树的叶节点是基于用户的身份内容信息与其他数据信息而编码生成的；

[49]所述发送单元还用于：向所述存储终端发送所述其他数据信息与所述叶节点的对应20 关系。

[50]更优地，所述其他数据信息为随机数。

[51]更优地，所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。

[52]更优地，所述存储终端包括认证机构的服务器；

25 [53]所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中；

[54]其中，所述数字证书包括内容部分与签名部分，所述内容部分包括基于用户的多个

身份信息内容构建的默克尔树的根值，所述签名部分是对所述内容部分的电子签名。

[55]更优地，所述数字证书的内容部分还包括所述用户的多个身份信息内容与所述叶节点的对应关系、和所述用户的多个身份信息内容对应的叶节点在基于用户的多个身份信息内容构建的默克尔树上的默克尔证明。

- 5 [56]更优地，所述存储终端还包括用户的客户端或区块链的分布式数据库，所述用户的多个身份信息内容与所述叶节点的对应关系、和所述用户的多个身份信息内容对应的叶节点在基于用户的多个身份信息内容构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。

[57]更优地，所述用户的数字证书的内容部分还包括所述用户的公钥。

- 10 [58]本说明书还提供了一种用户的身份信息内容的验证装置，包括：

[59]获取单元，响应于待验证的身份信息内容，根据所述待验证的身份信息内容与基于用户的多个身份信息内容构建的默克尔树的叶节点的对应关系，从存储终端获取所述待验证的身份信息内容对应的叶节点的默克尔证明，及所述基于用户的多个身份信息内容构建的默克尔树的根值，其中，所述默克尔树的叶节点是基于所述用户的身份信息内容编码生成的；

- 15

[60]计算单元，基于所述待验证的身份信息内容和所述默克尔证明，计算所述待验证的身份信息内容对应的默克尔树的根值；

[61]对比确定单元，确定所述待验证的身份信息内容对应的默克尔树的根值与所述基于用户的多个身份信息内容构建的默克尔树的根值是否相同。

- 20 [62]更优地，所述默克尔树的叶节点是基于用户的身份信息内容与其他数据信息而编码生成的；

[63]所述获取单元还用于：从所述存储终端获取所述其他数据信息与所述叶节点的对应关系；

[64]所述计算单元：

- 25 [65]基于所述待验证的身份信息内容、所述其他数据信息和所述默克尔证明，计算所述待验证的身份信息内容对应的默克尔树的根值。

[66]更优地，所述其他数据信息为随机数。

[67]更优地，所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数

数据库中的一个或多个。

[68]更优地，所述存储终端包括认证机构的服务器；

[69]所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中，其中，所述数字证书包括内容部分与签名部分，所述内容部分包  
5 括基于用户的多个身份内容信息构建的默克尔树的根值，所述签名部分是对所述内容部分的电子签名；

[70]所述获取单元：

[71]获取所述用户的数字证书；

[72]利用所述数字证书的认证机构对应的公钥验签所述数字证书；

10 [73]在所述验签通过后，获取所述基于用户的多个身份内容信息构建的默克尔树的根值。

[74]更优地，所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明；

[75]所述获取单元：

15 [76]获取所述用户的数字证书；

[77]利用所述数字证书的认证机构对应的公钥验签所述数字证书；

[78]在所述验签通过后，获取待验证的身份内容信息与所述叶节点的对应关系，根据所述待验证的身份内容信息与所述叶节点的对应关系，获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。

20 [79]更优地，所述存储终端还包括用户的客户端或区块链的分布式数据库，所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。

[80]更优地，所述用户的数字证书的内容部分还包括所述用户的公钥。

25 [81]相应地，本说明书还提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述的用户的身份内容信息认证方法。

[82]相应地，本说明书还提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述的用户的身份内容信息验证方法。

[83]相应地，本说明书还提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述的用户的身份内容信息认证方法。

[84]相应地，本说明书还提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述的用户的身份内容信息验证方法。

[85]现有的数字证书内包含用户全部身份内容信息的明文或编码后的全部身份内容信息，验证机构在获取用户的数字证书后可以获知或通过解码获知用户的全部身份内容信息，易引发不必要的身份内容信息泄露。本说明书各实施例提供的用户的身份内容信息的认证、验证方法和装置，基于用户的多个身份内容信息构建默克尔树，通过上述默克尔树的根值保证经认证的任何一个身份内容信息不被篡改；利用待验证身份内容信息的默克尔证明与待验证身份内容信息生成默克尔树的根值的方式，来校验待验证身份信息是否验证通过；从而使验证机构在对用户的身份验证时，仅获知用户待验证的身份信息或与待验证的身份信息相关的身份信息，而不能获取用户全部的身份信息，由此防止了以上提及的不必要的身份内容信息泄露的问题，更加提高了用户的身份内容信息验证过程的安全性。

#### 附图说明

[86]图 1 为本说明书一示例性实施例提供的用户的身份内容信息的认证、验证方法流程图；

[87]图 2 为本说明书一示例性实施例提供的基于用户的多个身份内容信息构建的默克尔树的示意图；

[88]图 3 为本说明书一示例性实施例提供的用户的身份内容信息的认证装置的示意图；

[89]图 4 为本说明书一示例性实施例提供的用户的身份内容信息的验证装置的示意图；

[90]图 5 为运行本说明书所提供的用户的身份内容信息的认证或验证装置实施例的一种硬件结构图。

## 具体实施方式

[91]数字证书是一个经身份认证机构数字签名的、包含用户身份内容信息（通常为用户的公钥、名称、身份代码等）的文件。它是能提供在互联网上进行身份验证的一种权威性电子文档，人们可以在互联网交往中，例如，在发送安全电子邮件、访问安全站点、  
5 网上证券交易、网上招标采购、网上办公、网上保险、网上税务、网上签约和网上银行等安全电子事务处理和安全电子交易活动中，用它来证明自己的身份和识别对方的身份。

[92]身份认证机构，又称 CA 机构，在颁发数字证书时，通常将用户的多个身份内容信息，包括公钥、名称、身份号码（机构用户为社会统一信用代码或机构验证码，个人用户为身份证号码）、地址等，统一以明文的格式、或编码后的格式保存在数字证书中，  
10 在上述数字证书被验证时，上述数字证书内包含的全部身份信息均可被验证机构获得，而对上述全部身份信息的披露多数情况下是不必要的，例如，在利用电子商务购物时，买家用户的身份证号码、家庭住址、户口情况等信息一般无需披露给电商网站或卖家，但现在仍缺少一种可选择性地披露用户的身份内容信息的验证方法。

[93]上述基于数字证书的身份验证方式，通常用于互联网上的身份验证；对于线下的身份验证方式，一般利用国家权威机构颁发的身份证、营业执照等实行，同样，个人的身份证（或户口本）、公司机构的营业执照（或组织机构代码证书）均包含很多身份内容信息，而且多数身份内容信息为隐私信息不便随意透露，现在也仍缺少一种可线下实行的、选择性地披露用户的身份内容信息的验证方法。

[94]为解决如上所述的问题，图 1 示意了本说明书一示意性实施例提供的用户的身份内容信息的认证、验证方法流程示意图。用于对用户的身份内容信息进行认证的机构，所执行的步骤包括：

[95]步骤 102，获取用户的多个身份内容信息。

[96]本说明书上述实施例所述的“用户”可包括个人用户及机构用户，还可包括计算机设备及在网络通信中涉及到的其他终端设备或如网页等个体等，在本说明书中不作限定，  
25 无论线上还是线下，任何需要验证身份的个体均可为本说明书所述的用户。

[97]本说明书上述实施例所述的用户的多个身份内容信息，可包括用户的姓名、身份证号码、地址，或机构用户的机构名称、代码、地址、法人信息等，对于网页个体，还可包括网页的服务器名称、IP 地址等。公钥作用一项重要的身份内容信息，在线上的各种应用场景中代表用户身份被广泛使用，因此上述实施例所述的用户的多个身份内容信息

还可包括用户的公钥。公钥（或称“公开密钥”）是与用户的私钥对应的，由私钥按照预设的加密算法得出，加密算法可包括 RSA、ECC 等。

[98]在向身份认证机构申请身份认证时，用户将自身需认证的多个身份内容信息发送给认证机构的服务器。认证机构的后台数据库在接收到上述多个身份内容信息后，通常会  
5 对上述信息的真实有效性进行核验，在核验完毕后即认证上述多个身份内容信息为有效的信息。

[99]步骤 104，基于所述用户的多个身份内容信息构建默克尔树，所述默克尔树的叶节点是基于所述用户的身份内容信息而编码生成的；

[100] 认证机构在收到上述用户的多个身份内容信息后，或验明上述用户的多个身份  
10 内容信息的真实有效性后，会基于上述用户的多个身份内容信息构建默克尔树（Merkle Tree）。默克尔树是数据结构中的一种树，可以是二叉树，也可以是多叉树，图 2 为本说明书一示例性实施例提供的基于用户的多个身份内容信息构建的默克尔树的示意图。如图 2 所示，用户的多个身份内容信息 Data 001、Data 002、Data 003、Data 004 经过编  
15 码生成相应的多个数字摘要 hash(Data 001)、hash(Data 002)、hash(Data 003)、hash(Data 004)，并将该多个数字摘要作为该默克尔树的叶节点 C、D、E、F 的值。对叶节点两两继续进行编码计算，以逐级生成各非叶节点 A 和 B 的值 hash(C+D)、hash(E+F)；经过对非叶节点的逐层计算，最终可得到该默克尔树的根节点 root 的值（在本说明书中可简称“默克尔树的根值”），如图 2 所示，最终生成默克尔树的根值 hash(A+B)。

[101] 图 2 中采用哈希算法构建上述默克尔树，本领域的技术人员应知，构建默克尔  
20 树可采用的编码算法可包括哈希算法（如 MD5，SHA256 等）、或其他任意所需的编码算法（如 base 64 等）。由于哈希算法是单向映射算法，无法从哈希摘要反推回原始数据内容，因此为保护用户的多个身份内容信息的隐私性，本说明书提供的上述实施例优选利用哈希算法构建上述基于用户的多个身份内容信息的默克尔树，以防止由默克尔树的叶节点反推得到用户的身份内容信息的原始数据内容。另外值得注意的是，在上述默  
25 克尔树的形成过程中，既可对各层级节点选用相同的数学编码算法进行编码计算，也可对不同的层级选用不同的编码算法，在此不作限定。

[102] 在本说明书提供的实施例中，并限定生成每个叶节点所依据的用户的身份内  
30 容信息的个数，每个叶节点可基于一条身份内容信息编码生成，也可基于多条身份内容信息；而且，每个叶节点除包含用户的身份内容信息外，还可包含其他数据内容信息，在此不做限定。

[103] 步骤 106, 向存储终端发送所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明, 及所述基于用户的多个身份内容信息构建的默克尔树的根值。

[104] 从默克尔树中的任一节点出发, 到达默克尔树的根节点所经过的路径节点上存储的数据摘要, 可以构造一个默克尔证明。一个节点的默克尔证明可能有多条, 如图 2 所示, 叶节点 E 的默克尔证明可以是 {F,A}, 或者也可可是 {F, (C+D)}; 叶节点 E 依次与默克尔证明所包含的节点上存储的数据摘要进行编码计算, 最终应得到该默克尔树的根值。因此, 若要验证叶节点 E 所对应的身份内容信息 Data 003 是否被篡改, 只需将待验证的身份内容信息作编码计算, 并将上述编码计算的结果与叶节点 E 的默克尔证明 { F,A } 或 {F,(C+D)} 对应的数据摘要值依次作编码计算, 即可得到待验证的身份内容信息对应的默克尔树的根值, 将待验证的数据对应的默克尔树的根值与上述基于身份内容信息 Data 001、Data 002、Data 003、Data 004 构建的默克尔树的根值作对比, 如果两值相等, 则证明待验证的身份内容信息即为 Data 003。在上述验证 Data003 的过程中, 并不需要其他叶节点所对应的身份内容信息如 Data 001, Data 002, Data 004 的内容, 因此很好地避免了对用户其他身份内容信息的披露。

[105] 由上可知, 在本说明书提供的上述实施例中, 为了利用基于用户的多个身份内容信息构建的默克尔树来进行用户的身份内容信息验证, 认证机构需发送用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明, 及所述基于用户的多个身份内容信息构建的默克尔树的根值。其中, 对用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明, 及所述基于用户的多个身份内容信息构建的默克尔树的根值的发送方式, 可以以发送如图 2 所述的整个默克尔树的形式来实现; 当然, 也可以将每个叶节点对应的默克尔证明、及上述默克尔树的根值分别发送, 在此不做限定。

[106] 值得注意的是, 如果数据所对应的叶节点的位置发生改变, 例如图 2 所示的 Data 001 与 Data 002 的位置发生调换, 则叶节点 C 与 D 的值发生互换, 则节点 A 的值会发生改变, 最终根节点 Root 的值也会发生改变, 因此在说明书提供的实施例中, 为方便利用上述默克尔树对用户的身份内容信息进行验证, 用户的多个身份内容信息与默克尔树的叶节点的对应关系也应被发送。

[107] 对上述用户的多个身份内容信息与默克尔树的叶节点的对应关系的发送可以有

多种实现方式。例如，可直接将用户的身份内容信息与默克尔树的叶节点的对应关系以映射表格的形式发送；又如，为保护用户的身份内容信息的隐私性，可以将用户的身份内容信息按类别进行编号，将上述编号与默克尔树的叶节点的对应关系以映射表格的形式发送；又或者，认证机构可生成身份内容信息的认证模板，在上述模板上规定有上述默克尔树的每个叶节点应对应的身份内容信息的类别，则上述模板即是以一种公知的形式发送上述用户的多个身份内容信息与默克尔树的叶节点的对应关系。

[108] 基于以上的一个或多个实施例，如图 1 所示，通过认证机构对用户的多个身份内容信息的认证及基于上述用户的多个身份内容信息的默克尔树的构建，用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值被发送至存储终端。

[109] 值得注意的是，在本说明书提供的上述实施例所描述的基于用户的多个身份内容信息构建的默克尔树，通常可采用哈希摘要算法来生成。由于哈希摘要算法为单向映射算法，即使验证机构获取到上述默克尔树的所有叶节点的值，验证机构也无法获知生成所述叶节点的用户的身份内容信息的原文，从而保证了用户的身份内容信息的安全性。

[110] 当然，上述默克尔树的编码算法并不限于哈希算法，如果认证机构采用了非哈希算法构建上述默克尔树，尤其是采用了可反向解码的编码方法（如 base 64 等）构建上述默克尔树，为了进一步保证默克尔树所基于的用户的全部身份内容信息不被轻易获取，上述默克尔树的叶节点可基于用户的身份内容信息和随机数共同生成。在该实施方式中，认证机构还应发送所述随机数、与所述叶节点的对应关系，从而将与用户的身份内容信息及叶节点对应的随机数存储于存储终端。

[111] 另外，如果上述默克尔树的一个叶节点是由身份内容信息与其他数据信息经编码生成时，认证机构还应发送所述其他数据信息与所述叶节点的对应关系，从而将与用户的身份内容信息及叶节点对应的其他数据信息存储于存储终端。类似地，上述其他数据信息（如随机数）与所述叶节点的对应关系也可以有多种实现方式。例如，可直接将其他数据信息与默克尔树的叶节点的对应关系以映射表格的形式发送；又如，将其他数据信息按类别进行编号，将上述编号与默克尔树的叶节点的对应关系以映射表格的形式发送；又或者，认证机构可生成身份内容信息的认证模板，在上述模板上规定有上述默克尔树的每个叶节点应对应的身份内容信息的类别、及其他身份信息及其类别，则上述模板的确立即是以一种公知的形式发送上述用户的多个身份内容信息与默克尔树的叶

节点的对应关系。

[112] 至此，所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值被发送至存储终端；可选的，所述其他数据信息与所述叶节点的对应关系也被发送至存储终端。上述本说明书上述一个或多个实施例所述的存储终端可以有多种实现方式，例如可以为认证机构发出的数字证书、认证机构的服务器、用户的客户端、或公用的存证机构服务器、或区块链的分布式数据库等等，在本说明书中不作限定。

[113] 例如，在一示出的实施例中，上述存储终端为认证机构的服务器。为进一步表示认证机构对用户的多个身份内容信息的认可，认证机构可向用户颁发数据证书。数字证书通常包括内容部分和签名部分，认证机构可将上述基于用户的多个身份内容信息构建的默克尔树的根值存储于数字证书的内容部分，并使用认证机构的私钥对数字证书的内容部分进行电子签名，已完成对上述默克尔树的根值的存证。由上述实施例中描述的默克尔树的根值的计算过程可知，默克尔树的根值与任一叶节点的内容和位置都直接相关，任一叶节点的内容或位置的变更都会引起根值的改变。因此认证机构将上述默克尔树的根值存储于数字证书，并进一步通过数字签名技术保证了该根值的有效性和安全性，防止该根值被恶意篡改。

[114] 在又一示出的实施例中，上述数字证书的内容部分还可包括以上实施例所述的用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明；当所述叶节点是由用户的身份内容信息与其他数据信息（如随机数）编码生成时，上述数字证书的内容部分还可包括其他数据信息与叶节点的对应关系。这样用户仅仅通过向验证机构出示数字证书，即可完成对数字证书中所认证的任意的身份内容信息的验证，达到方便、安全、高效的目的。

[115] 在又一示出的实施例中，所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值，被存储于身份认证机构的服务器；当所述叶节点是由用户的身份内容信息与其他数据信息（如随机数）编码生成时，还应存储其他数据信息与叶节点的对应关系。由于身份认证机构通常是具备身份认证资质的公正权威机构，将上述经认证的用户的多个身份内容

信息、及上述身份内容验证过程所需的默克尔证明及默克尔树的根值（可以表现为整棵默克尔树）存储于身份认证机构，在验证机构对用户的任何身份内容进行验证时，从身份认证机构获取验证信息，可保证上述获取的验证信息的真实性。

[116] 在又一示出的实施例中，所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值，被存储于用户的客户端；当所述叶节点是由用户的身份内容信息与其他数据信息（如随机数）编码生成时，还应存储其他数据信息与叶节点的对应关系。相比于将上述信息存储于认证机构的服务器，本实施例所提供的实施方式极大地减轻了认证机构服务器的存储压力，但缺点是用户的客户端提供的数据不具备安全性和权威性，容易被用户篡改；因此本实施方式可以与将上述默克尔树的根值存储于数字证书中的实施方式配合使用，即验证机构可从经认证机构数字签名认可的数字证书中获取上述默克尔树的根值，从用户的客户端获取待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，既保证了所获数据的真实性，又缓解了认证机构服务器的存储压力。

[117] 在又一示出的实施例中，所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值，被存储于区块链的分布式数据库；当所述叶节点是由用户的身份内容信息与其他数据信息（如随机数）编码生成时，还应存储其他数据信息与叶节点的对应关系。

[118] 上述实施例所述的区块链，具体可指一个各节点通过共识机制达成的、具有分布式数据存储结构的 P2P 网络系统，该区块链内的数据分布在时间上相连的一个个“区块（block）”之内，后一区块包含前一区块的数据摘要，且根据具体的共识机制（如 POW、POS、DPOS 或 PBFT 等）的不同，达成全部或部分节点的数据全备份。本领域的技术人员熟知，由于区块链系统在相应共识机制下运行，已收录至区块链数据库内的数据很难被任意的节点篡改，例如采用 Pow 共识的区块链，至少需要全网 51%算力的攻击才有可能篡改已有数据，因此区块链系统有着其他中心化数据库系统所法比拟的保证数据安全、防攻击篡改的特性。由此可知，在本说明书所提供的实施例中，被收录至区块链的分布式数据库中的数据不会被攻击或篡改，从而保证了验证机构在对用户的一身份内容信息进行验证时所获数据的真实性。

[119] 类似的,上述区块链的分布式数据库与数字证书可以结合使用,将上述默克尔树的根值存证于数字证书中,即验证机构可从经认证机构数字签名认可的数字证书中获取上述默克尔树的根值,从区块链的分布式数据库中获取待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明,既保证了所获数据的真实性,又缓解了认证机构服务器的存储压力。

[120] 任何对用户的身份内容信息具有验证需求的机构(图1所示的验证机构),响应于待验证的身份内容信息,可执行以下步骤完成验证:

[121] 步骤202,从存储终端获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明,及所述基于用户的多个身份内容信息构建的默克尔树的根值。

[122] 对上述默克尔证明的获取方式,可以包括:根据存储终端存储的待验证的身份内容信息(或其类别)与叶节点的对应关系,获取待验证的身份内容信息所对应的叶节点,或者根据认证机构的身份内容信息的认证模板规定的身份内容信息类别与叶节点的对应关系、获取待验证的身份内容信息所对应的叶节点;

[123] 再从存储终端存储的默克尔树、或存储终端存储的每个叶节点的默克尔证明、及默克尔树的根值,获取待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明,及所述基于用户的多个身份内容信息构建的默克尔树的根值。

[124] 本领域的技术人员应知,当上述默克尔树的一个叶节点是由多个身份内容信息经编码计算生成、或是由待验证的身份内容信息与其他数据信息经编码生成时,上述验证机构还应获取与所述待验证的身份内容信息一起生成上述叶节点的其他内容信息。

[125] 值得注意的是,当上述存储终端为认证机构的服务器时,所述基于用户的多个身份内容信息构建的默克尔树的根值可被所述认证机构存证于所述用户的数字证书中;获取所述基于用户的多个身份内容信息构建的默克尔树的根的值,包括:获取所述用户的数字证书,其中所述数字证书包含内容部分和签名部分,所述内容部分包括所述基于用户的多个身份内容信息构建的默克尔树的根值,所述签名部分是所述数字证书的认证机构对所述内容部分的电子签名;利用所述数字证书的认证机构对应的公钥验签所述数字证书;在所述验签通过后,获取所述基于用户的多个身份内容信息构建的默克尔树的根值。

- [126] 可选的, 上述数字证书的内容部分还可包括有所述用户的身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。上述信息可以默克尔树的形式整体存在于上述数字证书中。相应地, 还可在上述数字证书验签通过后获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明, 包括: 获取待验证的身份内容信息与所述叶节点的对应关系, 根据所述待验证的身份内容信息与所述叶节点的对应关系, 获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。
- [127] 类似地, 上述存储终端还可以是认证机构的服务器、用户的客户端或区块链的分布式数据库, 以上的实施例中已详细论证, 在此不再赘述。
- [128] 步骤 204, 基于所述待验证的身份内容信息和所述默克尔证明, 计算所述待验证的身份内容信息对应的默克尔树的根值。
- [129] 上述步骤包括基于所述待验证的身份内容信息做编码计算以得到待验证的身份内容信息对应的数据摘要, 上述数据摘要作为待验证的默克尔树的叶节点的值, 再将上述数据摘要与上述待验证的身份内容信息对应的叶节点的默克尔证明包含的节点的值、依次作编码计算, 最终得出待验证的身份内容信息对应的默克尔树的根值。
- [130] 本领域的技术人员应知, 当上述默克尔树的一个叶节点是由多个身份内容信息经编码计算生成、或是由待验证的身份内容信息与其他数据信息(如随机数)经编码生成时, 上述基于所述待验证的身份内容信息做编码计算以得到待验证的身份内容信息对应的数据摘要, 还应包括, 将所述待验证的身份内容信息与其他内容信息一起做编码计算, 以得到待验证的身份内容信息对应的数据摘要。
- [131] 步骤 206, 确定所述待验证的身份内容信息对应的默克尔树的根值与所述基于用户的多个身份内容信息构建的默克尔树的根值是否相同。
- [132] 对比上述待验证的身份内容信息对应的默克尔树的根值与存储终端存储的默克尔树的根值是否相同; 如果相同, 则上述待验证的身份内容信息通过验证, 及上述待验证的身份内容信息为上述认证机构认可的身份内容信息。
- [133] 由此可知, 通过图 1 所示的用户的身份内容信息的认证、验证方法, 用户可以在不披露其他身份内容信息的前提下获得待验证信息的验证, 从而提高了用户的身份内容信息验证过程的安全性; 而且, 在上述验证的过程中, 仅传输待验证的身份内容信息

的默克尔证明、及默克尔树的根值，相比传统的验证方法，减小了数据的传输量，提高了验证的效率。上述对用户的身份内容信息的认证、验证方法，不仅限于线上的数据传输、支付等场景下的身份验证时使用，用户在线下的场景中仍可使用，例如用户到宾馆入住，宾馆可通过从存储终端获取相应信息的方式完成对用户身份的验证，因此上述方法具有广泛的应用场景。

[134] 本说明书提供的上述实施例所描述的用户的身​​份内容信息通常可包括用户的公钥、用户的名称、用户的地址、用户的识别号码等信息中的一种或多种等，其中，用户的公钥作为常用的信息在互联网上被广泛的使用，例如，作为用户身份的代表、或在传输信息解密、电子签名验签等场景中被广泛使用；且公钥信息作为一串字符编码由于不揭露用户的隐私而可被广泛告知，因此，在本说明书提供的一种优选的实施方式中，可以将公钥与基于用户的多个身份内容信息生成的默克尔树的根值保存于本说明书所提供的数字证书的内容部分，这样验证机构可通过验签数字证书的签名后直接获取用户的公钥，用于信息解密或用户的电子签名验签等场景中。

[135] 与上述流程实现对应，本说明书的实施例还提供了一种用户的身​​份内容信息的认证装置、及用户的身​​份内容信息的验证装置。上述各装置可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为逻辑意义上的装置，是通过所在设备的 CPU(Central Process Unit, 中央处理器)将对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，除了图 5 所示的 CPU、内存以及存储器之外，上述各装置所在的设备通常还包括用于进行无线信号收发的芯片等其他硬件，和/或用于实现网络通信功能的板卡等其他硬件。

[136] 图 3 所示为本说明书所提供的一种用户的身​​份内容信息的认证装置 30，包括：

[137] 获取单元 302，获取用户的多个身份内容信息；

[138] 默克尔树构建单元 304，基于所述用户的多个身份内容信息构建默克尔树，所述默克尔树的叶节点是基于所述用户的身​​份内容信息编码生成的；

[139] 发送单元 306，向存储终端发送所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值。

[140] 更优地，所述默克尔树的叶节点是基于用户的身​​份内容信息与其他数据信息而

编码生成的;

[141] 所述发送单元 306 还用于: 向所述存储终端发送所述其他数据信息与所述叶节点的对应关系。

[142] 更优地, 所述其他数据信息为随机数。

5 [143] 更优地, 所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。

[144] 更优地, 所述存储终端包括认证机构的服务器;

[145] 所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中;

10 [146] 其中, 所述数字证书包括内容部分与签名部分, 所述内容部分包括基于用户的多个身份内容信息构建的默克尔树的根值, 所述签名部分是对所述内容部分的电子签名。

[147] 更优地, 所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。

15 [148] 更优地, 所述存储终端还包括用户的客户端或区块链的分布式数据库, 所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。

[149] 更优地, 所述用户的数字证书的内容部分还包括所述用户的公钥。

20 [150] 相应的, 如图 4 所示, 本说明书还提供了一种用户的身份内容信息的验证装置 40, 包括:

[151] 获取单元 402, 响应于待验证的身份内容信息, 根据所述待验证的身份内容信息与基于用户的多个身份内容信息构建的默克尔树的叶节点的对应关系, 从存储终端获取所述待验证的身份内容信息对应的叶节点的默克尔证明, 及所述基于用户的多个身份内容信息构建的默克尔树的根值, 其中, 所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的;

25

[152] 计算单元 404, 基于所述待验证的身份内容信息和所述默克尔证明, 计算所述待验证的身份内容信息对应的默克尔树的根值;

- [153] 对比确定单元 406, 确定所述待验证的身份内容信息对应的默克尔树的根值与所述基于用户的多个身份内容信息构建的默克尔树的根值是否相同。
- [154] 更优地, 所述默克尔树的叶节点是基于用户的身份内容信息与其他数据信息而编码生成的;
- 5 [155] 所述获取单元 402 还用于: 从所述存储终端获取所述其他数据信息与所述叶节点的对应关系;
- [156] 所述计算单元 404:
- [157] 基于所述待验证的身份内容信息、所述其他数据信息和所述默克尔证明, 计算所述待验证的身份内容信息对应的默克尔树的根值。
- 10 [158] 更优地, 所述其他数据信息为随机数。
- [159] 更优地, 所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。
- [160] 更优地, 所述存储终端包括认证机构的服务器;
- [161] 所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中, 其中, 所述数字证书包括内容部分与签名部分, 所述内容部分包括基于用户的多个身份内容信息构建的默克尔树的根值, 所述签名部分是对所述内容部分的电子签名;
- 15 [162] 所述获取单元 402:
- [163] 获取所述用户的数字证书;
- 20 [164] 利用所述数字证书的认证机构对应的公钥验签所述数字证书;
- [165] 在所述验签通过后, 获取所述基于用户的多个身份内容信息构建的默克尔树的根值。
- [166] 更优地, 所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明;
- 25 [167] 所述获取单元 402:
- [168] 获取所述用户的数字证书;

- [169] 利用所述数字证书的认证机构对应的公钥验签所述数字证书;
- [170] 在所述验签通过后, 获取待验证的身份内容信息与所述叶节点的对应关系, 根据所述待验证的身份内容信息与所述叶节点的对应关系, 获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。
- 5 [171] 更优地, 所述存储终端还包括用户的客户端或区块链的分布式数据库, 所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。
- [172] 更优地, 所述用户的数字证书的内容部分还包括所述用户的公钥。
- 10 [173] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程, 相关之处参见方法实施例的部分说明即可, 在此不再赘述。
- [174] 以上所描述的装置实施例仅仅是示意性的, 其中所述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或者也可以不是物理模块, 即可以位于一个地方, 或者也可以分布到多个网络模块上。可以根据实际的需要
- 15 选择其中的部分或者全部单元或模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下, 即可以理解并实施。
- [175] 上述实施例阐明的装置、单元、模块, 具体可以由计算机芯片或实体实现, 或者由具有某种功能的产品来实现。一种典型的实现设备为计算机, 计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体
- 20 体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。
- [176] 与上述方法实施例相对应, 本说明书的实施例还提供了一种计算机设备, 该计算机设备包括存储器和处理器。其中, 存储器上存储有能够由处理器运行的计算机程序; 处理器在运行存储的计算机程序时, 执行本说明书实施例中用户的身份内容信息认证方
- 25 法的各个步骤。对上述用户的身份内容信息认证方法的各个步骤的详细描述请参见之前的内容, 不再重复。
- [177] 与上述方法实施例相对应, 本说明书的实施例还提供了一种计算机设备, 该计算机设备包括存储器和处理器。其中, 存储器上存储有能够由处理器运行的计算机程序; 处理器在运行存储的计算机程序时, 执行本说明书实施例中用户的身份内容信息验证方

法的各个步骤。对上述用户的身份内容信息验证方法的各个步骤的详细描述请参见之前的内容，不再重复。

[178] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机可读存储介质，该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例5中用户的身份内容信息认证方法的各个步骤。对用户的身份内容信息认证方法的各个步骤的详细描述请参见之前的内容，不再重复。

[179] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机可读存储介质，该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例10中用户的身份内容信息验证方法的各个步骤。对用户的身份内容信息验证方法的各个步骤的详细描述请参见之前的内容，不再重复。

[180] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

[181] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。15

[182] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[183] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。20

[184] 计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，25 磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[185] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排

他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

- 5 [186] 本领域技术人员应明白,本说明书的实施例可提供为方法、系统或计算机程序产品。因此,本说明书的实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且,本说明书的实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

### 权利要求书

- 1、一种用户的身份内容信息的认证方法，包括：  
获取用户的多个身份内容信息；  
基于所述用户的多个身份内容信息构建默克尔树，所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的；  
向存储终端发送所述用户的多个身份内容信息与所述叶节点的对应关系，所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值。
- 2、根据权利要求 1 所述的方法，所述默克尔树的叶节点是基于用户的身份内容信息与其他数据信息而编码生成的；  
所述方法还包括：向所述存储终端发送所述其他数据信息与所述叶节点的对应关系。
- 3、根据权利要求 2 所述的方法，所述其他数据信息为随机数。
- 4、根据权利要求 1 至 3 中任一权利要求所述的方法，所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。
- 5、根据权利要求 1 至 3 中任一权利要求所述的方法，所述存储终端包括认证机构的服务器；  
所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中；  
其中，所述数字证书包括内容部分与签名部分，所述内容部分包括基于用户的多个身份内容信息构建的默克尔树的根值，所述签名部分是对所述内容部分的电子签名。
- 6、根据权利要求 5 所述的方法，所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。
- 7、根据权利要求 5 所述的方法，所述存储终端还包括用户的客户端或区块链的分布式数据库，所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。
- 8、根据权利要求 5 所述的方法，所述用户的数字证书的内容部分还包括所述用户的公钥。
- 9、根据权利要求 1 所述的方法，所述用户的身份内容信息包括用户的公钥、用户的名称、用户的地址、用户的识别号码中的一种或多种。

10、根据权利要求 1 至 3 中任一权利要求所述的方法，所述编码包括哈希编码。

11、一种用户的身份内容信息的验证方法，包括：

响应于待验证的身份内容信息，根据所述待验证的身份内容信息与基于用户的多个身份内容信息构建的默克尔树的叶节点的对应关系，从存储终端获取所述待验证的身份内容信息对应的叶节点的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值，其中，所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的；

基于所述待验证的身份内容信息和所述默克尔证明，计算所述待验证的身份内容信息对应的默克尔树的根值；

确定所述待验证的身份内容信息对应的默克尔树的根值与所述基于用户的多个身份内容信息构建的默克尔树的根值是否相同。

12、根据权利要求 11 所述的方法，所述默克尔树的叶节点是基于用户的身份内容信息与其他数据信息而编码生成的；

所述方法还包括：从所述存储终端获取所述其他数据信息与所述叶节点的对应关系；

所述基于所述待验证的身份内容信息和所述默克尔证明，计算所述待验证的身份内容信息对应的默克尔树的根值，包括：

基于所述待验证的身份内容信息、所述其他数据信息和所述默克尔证明，计算所述待验证的身份内容信息对应的默克尔树的根值。

13、根据权利要求 12 所述的方法，所述其他数据信息为随机数。

14、根据权利要求 11 至 13 中任一权利要求所述的方法，所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。

15、根据权利要求 11 至 13 中任一权利要求所述的方法，所述存储终端包括认证机构的服务器；

所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中，其中，所述数字证书包括内容部分与签名部分，所述内容部分包括基于用户的多个身份内容信息构建的默克尔树的根值，所述签名部分是对所述内容部分的电子签名；

所述从存储终端获取所述基于用户的多个身份内容信息构建的默克尔树的根值，包括：

获取所述用户的数字证书；

30 利用所述数字证书的认证机构对应的公钥验签所述数字证书；

在所述验签通过后，获取所述基于用户的多个身份内容信息构建的默克尔树的根值。

16、根据权利要求 15 所述的方法，所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明；

所述从存储终端获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，包括：

获取所述用户的数字证书；

利用所述数字证书的认证机构对应的公钥验签所述数字证书；

在所述验签通过后，获取待验证的身份内容信息与所述叶节点的对应关系，根据所述待验证的身份内容信息与所述叶节点的对应关系，获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。

17、根据权利要求 15 所述的方法，所述存储终端还包括用户的客户端或区块链的分布式数据库，所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。

18、根据权利要求 15 所述的方法，所述用户的数字证书的内容部分还包括所述用户的公钥。

19、根据权利要求 11 所述的方法，所述用户的身份内容信息包括用户的公钥、用户的名称、用户的地址、用户的识别号码中的一种或多种。

20、根据权利要求 11 至 13 中任一权利要求所述的方法，所述编码包括哈希编码。

21、一种用户的身份内容信息的认证装置，包括：

获取单元，获取用户的多个身份内容信息；

默克尔树构建单元，基于所述用户的多个身份内容信息构建默克尔树，所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的；

发送单元，向存储终端发送所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值。

22、根据权利要求 21 所述的装置，所述默克尔树的叶节点是基于用户的身份内容信息与其他数据信息而编码生成的；

所述发送单元还用于：向所述存储终端发送所述其他数据信息与所述叶节点的对应关系。

23、根据权利要求 22 所述的装置，所述其他数据信息为随机数。

24、根据权利要求 21 至 23 中任一权利要求所述的装置，所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。

25、根据权利要求 21 至 23 中任一权利要求所述的装置，所述存储终端包括认证机构的服务器；

5        所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中；

其中，所述数字证书包括内容部分与签名部分，所述内容部分包括基于用户的多个身份内容信息构建的默克尔树的根值，所述签名部分是对所述内容部分的电子签名。

26、根据权利要求 25 所述的装置，所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。

27、根据权利要求 25 所述的装置，所述存储终端还包括用户的客户端或区块链的分布式数据库，所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。

28、根据权利要求 25 所述的装置，所述用户的数字证书的内容部分还包括所述用户的公钥。

29、一种用户的身份内容信息的验证装置，包括：

获取单元，响应于待验证的身份内容信息，根据所述待验证的身份内容信息与基于用户的多个身份内容信息构建的默克尔树的叶节点的对应关系，从存储终端获取所述待验证的身份内容信息对应的叶节点的默克尔证明，及所述基于用户的多个身份内容信息构建的默克尔树的根值，其中，所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的；

25        计算单元，基于所述待验证的身份内容信息和所述默克尔证明，计算所述待验证的身份内容信息对应的默克尔树的根值；

对比确定单元，确定所述待验证的身份内容信息对应的默克尔树的根值与所述基于用户的多个身份内容信息构建的默克尔树的根值是否相同。

30、根据权利要求 29 所述的装置，所述默克尔树的叶节点是基于用户的身份内容信息与其他数据信息而编码生成的；

30        所述获取单元还用于：从所述存储终端获取所述其他数据信息与所述叶节点的对应关系；

所述计算单元:

基于所述待验证的身份内容信息、所述其他数据信息和所述默克尔证明, 计算所述待验证的身份内容信息对应的默克尔树的根值。

31、根据权利要求 30 所述的装置, 所述其他数据信息为随机数。

5 32、根据权利要求 29 至 31 中任一权利要求所述的装置, 所述存储终端包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。

33、根据权利要求 29 至 31 中任一权利要求所述的装置, 所述存储终端包括认证机构的服务器;

10 所述基于用户的多个身份内容信息构建的默克尔树的根值被所述认证机构存证于所述用户的数字证书中, 其中, 所述数字证书包括内容部分与签名部分, 所述内容部分包括基于用户的多个身份内容信息构建的默克尔树的根值, 所述签名部分是对所述内容部分的电子签名;

所述获取单元:

获取所述用户的数字证书;

15 利用所述数字证书的认证机构对应的公钥验签所述数字证书;

在所述验签通过后, 获取所述基于用户的多个身份内容信息构建的默克尔树的根值。

34、根据权利要求 33 所述的装置, 所述数字证书的内容部分还包括所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明;

20 所述获取单元:

获取所述用户的数字证书;

利用所述数字证书的认证机构对应的公钥验签所述数字证书;

25 在所述验签通过后, 获取待验证的身份内容信息与所述叶节点的对应关系, 根据所述待验证的身份内容信息与所述叶节点的对应关系, 获取所述待验证的身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明。

35、根据权利要求 33 所述的装置, 所述存储终端还包括用户的客户端或区块链的分布式数据库, 所述用户的多个身份内容信息与所述叶节点的对应关系、和所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明被存储于所述用户的客户端或所述区块链的分布式数据库。

30 36、根据权利要求 33 所述的装置, 所述用户的数字证书的内容部分还包括所述用户的公钥。

37、一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 1 到 10 任意一项所述的方法。

38、一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 11 到 20 任意一项所述的方法。

39、一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求 1 到 10 任意一项所述的方法。

40、一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求 11 到 20 任意一项所述的方法。