(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109583219 A
(43)申请公布日 2019.04.05

(21)申请号 201811455351.6

(22)申请日 2018.11.30

(71)申请人 国家电网有限公司
地址 100031 北京市西城区西长安街86号
申请人 国网电子商务有限公司
国网雄安金融科技有限公司

(72)发明人 樊涛 朱兴雄 贺金红 王俊生
杨珂 玄佳兴 韩文慧 吕梓童

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王宝筠

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/64(2013.01)

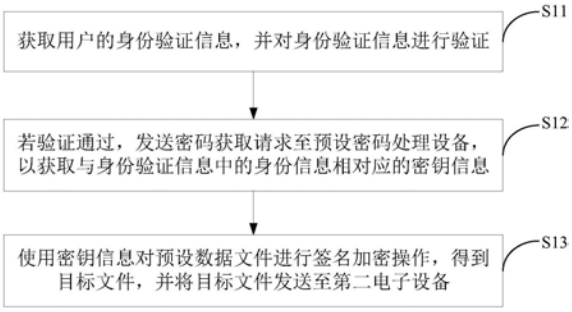
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种数据签名、加密及保存的方法、装置和设备

(57)摘要

本发明提供了一种数据签名、加密及保存的方法、装置和设备，本发明中，获取用户的身份验证信息，并对所述身份验证信息进行验证，若验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息；使用所述密钥信息对预设数据文件进行签名加密操作，得到目标文件，并将所述目标文件发送至第二电子设备，将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证。通过本发明实施例，将数据文件保存在区块链中，区块链本身具有数据防篡改功能，进而能够提高数据安全性。



CN 109583219 A

1.一种数据签名、加密及保存的方法，其特征在于，应用于第一电子设备，包括：

获取用户的身份验证信息，并对所述身份验证信息进行验证；

若验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息；所述密码获取请求包括所述身份信息；

使用所述密钥信息对预设数据文件进行签名加密操作，得到目标文件，并将所述目标文件发送至第二电子设备；

将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证。

2.根据权利要求1所述的方法，其特征在于，使用所述密钥信息对预设数据文件进行签名加密操作，包括：

使用所述密钥信息中的公钥信息，对预设数据文件进行加密操作；

使用所述密钥信息中的私钥信息，对进行加密操作后的预设数据文件进行签名操作。

3.一种数据签名、加密及保存的方法，其特征在于，应用于第二电子设备，包括：

接收第一电子设备发送的目标文件、获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件；

根据所述密钥信息，从所述目标文件中确定初始数据文件；

计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值；

依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

4.根据权利要求3所述的方法，其特征在于，根据所述密钥信息，从所述目标文件中确定初始数据文件，包括：

使用所述密钥信息中的私钥信息，对所述目标文件进行签名验证操作；

若签名验证操作成功，使用所述密钥信息中的公钥信息，对进行签名验证操作后的目标文件进行解密操作，得到所述初始数据文件。

5.根据权利要求3所述的方法，其特征在于，依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果，包括：

若相同，则确定所述目标文件未被篡改；

若不相同，则确定所述目标文件被篡改。

6.一种数据签名、加密及保存的装置，其特征在于，应用于第一电子设备，包括：

数据验证模块，用于获取用户的身份验证信息，并对所述身份验证信息进行验证；

请求发送模块，用于若验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息；所述密码获取请求包括所述身份信息；

数据处理模块，用于使用所述密钥信息对预设数据文件进行签名加密操作，得到目标文件，并将所述目标文件发送至第二电子设备；

数据保存模块，用于将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证。

7.根据权利要求6所述的装置，其特征在于，所述数据处理模块包括：

第一处理子模块，用于使用所述密钥信息中的公钥信息，对预设数据文件进行加密操

作；

第二处理子模块，用于使用所述密钥信息中的私钥信息，对进行加密操作后的预设数据文件进行签名操作。

8.一种数据签名、加密及保存的装置，其特征在于，应用于第二电子设备，包括：

数据获取模块，用于接收第一电子设备发送的目标文件、获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件；

文件确定模块，用于根据所述密钥信息，从所述目标文件中确定初始数据文件；

计算模块，用于计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值；

结果确定模块，用于依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

9.根据权利要求8所述的装置，其特征在于，所述文件确定模块包括：

第三处理子模块，用于使用所述密钥信息中的私钥信息，对所述目标文件进行签名验证操作；

第四处理子模块，用于若签名验证操作成功，使用所述密钥信息中的公钥信息，对进行签名验证操作后的目标文件进行解密操作，得到所述初始数据文件。

10.根据权利要求8所述的装置，其特征在于，所述结果确定模块包括：

第一确定子模块，用于若所述第一哈希值与所述第二哈希值相同，则确定所述目标文件未被篡改；

第二确定子模块，用于若所述第一哈希值与所述第二哈希值不相同，则确定所述目标文件被篡改。

11.一种电子设备，其特征在于，包括：处理器和发送端口；

其中，所述处理器，用于获取用户的身份验证信息，并对所述身份验证信息进行验证，使用密钥信息对预设数据文件进行签名加密操作，得到目标文件，将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证；

所述发送端口，用于若所述处理器对身份验证信息验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息，并将所述目标文件发送至第二电子设备；所述密码获取请求包括所述身份信息。

12.一种电子设备，其特征在于，包括：处理器和接收端口；

所述接收端口，用于接收第一电子设备发送的目标文件；

所述处理器，用于获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件，根据所述密钥信息，从所述目标文件中确定初始数据文件，计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值，依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

一种数据签名、加密及保存的方法、装置和设备

技术领域

[0001] 本发明涉及数据处理领域，更具体的说，涉及一种数据签名、加密及保存的方法、装置和设备。

背景技术

[0002] 电子设备，如计算机在进行数据处理时，会使用到数据，数据一般存储在数据库中，如将电商交易数据、合同等数据存储在数据库中。

[0003] 但是将数据存储在数据库中，很容易被篡改，安全性较低。

发明内容

[0004] 有鉴于此，本发明提供一种数据签名、加密及保存的方法、装置和设备，以解决将数据存储在数据库中，很容易被篡改，安全性较低的问题。

[0005] 为解决上述技术问题，本发明采用了如下技术方案：

[0006] 一种数据签名、加密及保存的方法，应用于第一电子设备，包括：

[0007] 获取用户的身份验证信息，并对所述身份验证信息进行验证；

[0008] 若验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息；所述密码获取请求包括所述身份信息；

[0009] 使用所述密钥信息对预设数据文件进行签名加密操作，得到目标文件，并将所述目标文件发送至第二电子设备；

[0010] 将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证。

[0011] 优选地，使用所述密钥信息对预设数据文件进行签名加密操作，包括：

[0012] 使用所述密钥信息中的公钥信息，对预设数据文件进行加密操作；

[0013] 使用所述密钥信息中的私钥信息，对进行加密操作后的预设数据文件进行签名操作。

[0014] 一种数据签名、加密及保存的方法，应用于第二电子设备，包括：

[0015] 接收第一电子设备发送的目标文件、获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件；

[0016] 根据所述密钥信息，从所述目标文件中确定初始数据文件；

[0017] 计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值；

[0018] 依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

[0019] 优选地，根据所述密钥信息，从所述目标文件中确定初始数据文件，包括：

[0020] 使用所述密钥信息中的私钥信息，对所述目标文件进行签名验证操作；

[0021] 若签名验证操作成功，使用所述密钥信息中的公钥信息，对进行签名验证操作后的目标文件进行解密操作，得到所述初始数据文件。

[0022] 优选地，依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果，包括：

[0023] 若相同，则确定所述目标文件未被篡改；

[0024] 若不相同，则确定所述目标文件被篡改。

[0025] 一种数据签名、加密及保存的装置，应用于第一电子设备，包括：

[0026] 数据验证模块，用于获取用户的身份验证信息，并对所述身份验证信息进行验证；

[0027] 请求发送模块，用于若验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息；所述密码获取请求包括所述身份信息；

[0028] 数据处理模块，用于使用所述密钥信息对预设数据文件进行签名加密操作，得到目标文件，并将所述目标文件发送至第二电子设备；

[0029] 数据保存模块，用于将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证。

[0030] 优选地，所述数据处理模块包括：

[0031] 第一处理子模块，用于使用所述密钥信息中的公钥信息，对预设数据文件进行加密操作；

[0032] 第二处理子模块，用于使用所述密钥信息中的私钥信息，对进行加密操作后的预设数据文件进行签名操作。

[0033] 一种数据签名、加密及保存的装置，应用于第二电子设备，包括：

[0034] 数据获取模块，用于接收第一电子设备发送的目标文件、获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件；

[0035] 文件确定模块，用于根据所述密钥信息，从所述目标文件中确定初始数据文件；

[0036] 计算模块，用于计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值；

[0037] 结果确定模块，用于依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

[0038] 优选地，所述文件确定模块包括：

[0039] 第三处理子模块，用于使用所述密钥信息中的私钥信息，对所述目标文件进行签名验证操作；

[0040] 第四处理子模块，用于若签名验证操作成功，使用所述密钥信息中的公钥信息，对进行签名验证操作后的目标文件进行解密操作，得到所述初始数据文件。

[0041] 优选地，所述结果确定模块包括：

[0042] 第一确定子模块，用于若所述第一哈希值与所述第二哈希值相同，则确定所述目标文件未被篡改；

[0043] 第二确定子模块，用于若所述第一哈希值与所述第二哈希值不相同，则确定所述目标文件被篡改。

[0044] 一种电子设备，包括：处理器和发送端口；

[0045] 其中，所述处理器，用于获取用户的身份验证信息，并对所述身份验证信息进行验证，使用密钥信息对预设数据文件进行签名加密操作，得到目标文件，将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证；

[0046] 所述发送端口，用于若所述处理器对身份验证信息验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息，并将所述目标文件发送至第二电子设备；所述密码获取请求包括所述身份信息。

[0047] 一种电子设备，包括：处理器和接收端口；

[0048] 所述接收端口，用于接收第一电子设备发送的目标文件；

[0049] 所述处理器，用于获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件，根据所述密钥信息，从所述目标文件中确定初始数据文件，计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值，依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

[0050] 相较于现有技术，本发明具有以下有益效果：

[0051] 本发明提供了一种数据签名、加密及保存的方法、装置及电子设备，本发明中，数据文件保存在区块链中，区块链本身具有数据防篡改功能，进而能够提高数据安全性。

附图说明

[0052] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0053] 图1为本发明实施例提供的一种应用于第一电子设备的数据签名、加密及保存的方法的方法流程图；

[0054] 图2为本发明实施例提供的另一种应用于第一电子设备的数据签名、加密及保存的方法的方法流程图；

[0055] 图3为本发明实施例提供的一种应用于第二电子设备的数据签名、加密及保存的方法的方法流程图；

[0056] 图4为本发明实施例提供的一种应用于第一电子设备的数据签名、加密及保存的装置的结构示意图；

[0057] 图5为本发明实施例提供的一种应用于第二电子设备的数据签名、加密及保存的装置的结构示意图。

具体实施方式

[0058] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0059] 本发明实施例提供了一种数据签名、加密及保存的方法，应用于第一电子设备，第一电子设备可以是手机、平板、笔记本等设备。本发明中的数据签名、加密及保存的方法主要针对的是各种合同数据、票据数据等，如光伏云签约合同、电商合同、光伏电网申请合同等。

[0060] 参照图1，数据签名、加密及保存的方法可以包括：

[0061] S11、获取用户的身份验证信息，并对所述身份验证信息进行验证；

[0062] 其中，身份验证信息包括账号、密码、生物特征等，本发明实施例中可以仅验证一种身份验证信息，也可以根据需要进行多种身份验证，如同时进行指纹、账号密码验证。其中，生物特征包括指纹、面部、声音等特征。

[0063] 身份验证的过程采用常规验证技术即可，本发明实施例不做特殊要求。

[0064] S12、若验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息；

[0065] 所述密码获取请求包括所述身份信息。

[0066] 具体的，若身份验证通过，则第一电子设备会向预设密码处理设备请求获取与该用户对应的密钥信息。其中，密钥信息包括私钥和公钥，每一用户都有唯一对应的公钥和私钥，这些公钥和私钥保存在预设密码处理设备中。

[0067] 第一电子设备向预设密码处理设备发送的密码获取请求中包括身份验证信息中的身份信息，如身份证号、手机号、姓名等信息。

[0068] 需要说明的是，预设密码处理设备下发的密钥信息为SM9密钥，SM9是一种标识密码标准，相关标准为“GM/T 0044-2016SM9标识密码算法”。SM9主要用于用户的身份认证，在使用SM9密钥时，不需要使用数字证书，简化了数据验证过程。

[0069] S13、使用所述密钥信息对预设数据文件进行签名加密操作，得到目标文件，并将所述目标文件发送至第二电子设备；

[0070] 可选的，在本实施例的基础上，参照图2，步骤S13可以包括：

[0071] S21、使用所述密钥信息中的公钥信息，对预设数据文件进行加密操作；

[0072] S22、使用所述密钥信息中的私钥信息，对进行加密操作后的预设数据文件进行签名操作。

[0073] 具体的，电子签名是数据电文中以电子形式用于识别签名人身份并表明签名人认可其中内容的数据，是通过密码技术对电子文档的电子形式的签名。

[0074] 加密可以实现数据的真实性、完整性、私密性、不可抵赖性。

[0075] 密钥信息包括公钥和私钥，公钥加密，私钥签名，加密和签名的过程仍采用常规技术手段，加密和签名的过程为使用数据信封方式对预设数据文件进行封装。

[0076] 第一电子设备，对预设数据文件进行签名加密操作后，得到目标文件，将目标文件发送给第二电子设备，其中，第二电子设备为与第一电子设备进行数据交互的设备，如第一电子设备和第二电子设备可以是合同的甲方和乙方的电子设备，双方进行合同签订。

[0077] S14、将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证。

[0078] 具体的，区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链具有防篡改功能，将预设数据文件保存到区块链中，能够保证预

设数据文件不被篡改。区块链技术可实现操作的全网、全过程、全交易的数据记录，其记录不可篡改。所有数据被全网所有节点共同拥有，网络空间的信息更加透明、行为更加可追溯，从而实现完整合规的合同签署过程。

[0079] 另外，当第二电子设备接收到目标文件后，还能够根据区块链中保存的预设数据文件判断目标文件在传输过程中是否被黑客篡改。

[0080] 本发明实施例中，数据文件保存在区块链中，区块链本身具有数据防篡改功能，进而能够提高数据安全性。

[0081] 另外，基于区块链技术和SM9算法来实现电子合同的签署、重要文件的存证取证。SM9算法可以实现数据的真实性、完整性、私密性、不可抵赖性。区块链技术可实现操作的全网、全过程、全交易的数据记录，其记录不可篡改。所有数据被全网所有节点共同拥有，网络空间的信息更加透明、行为更加可追溯，从而实现完整合规的合同签署过程。本实施例中，利用密码算法实现用户身份认证，并将用户签名行为、合同签署，通过区块链的分布式节点，建立人、事件、时间、地点等签名行为的溯源，签名行为、重要文件摘要特征值全链公开、可监督、可追溯，利用区块链技术的防篡改和防抵赖，实现可靠电子签名。并在身份可信的基础上，进一步支撑区块链上各业务的真实、可信，为业务提供可信区块链技术服务。

[0082] 可选的，在上述应用于第一电子设备的数据签名、加密及保存的方法的实施例的基础上，本发明的另一实施例提供了一种数据签名、加密及保存的方法，应用于第二电子设备，第二电子设备可以是手机、平板、笔记本等设备。

[0083] 参照图2，数据签名、加密及保存的方法可以包括：

[0084] S31、接收第一电子设备发送的目标文件、获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件；

[0085] 具体的，密钥信息可以是从第一电子设备处获取，也可以是从预设密码处理设备处获取。

[0086] 第一电子设备和第二电子设备可以处于同一个区块链集群中，这样，第一电子设备和第二电子设备均可以访问该区块链，第二电子设备从区块链中获取到该预设数据文件。此外，预设数据文件也可以是其他与第一电子设备处于同一区块链集群中的设备发送给第二电子设备。

[0087] S32、根据所述密钥信息，从所述目标文件中确定初始数据文件；

[0088] 其中，初始数据文件为从所述目标文件中提取得到的原始文件。

[0089] S33、计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值；

[0090] 具体的，哈希值计算方式采用常规手段即可。

[0091] S34、依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

[0092] 可选的，在本实施例的基础上，步骤S34可以包括：

[0093] 若相同，则确定所述目标文件未被篡改，若不相同，则确定所述目标文件被篡改。

[0094] 具体的，由于区块链中的预设数据文件为原始文件，若第二电子设备从接收的目标文件中提取的初始数据文件未被篡改，则初始数据文件应与预设数据文件相同，则初始数据文件与预设数据文件分别计算得到的哈希值也相同。

[0095] 若第二电子设备从接收的目标文件中提取的初始数据文件被篡改，则初始数据文

件应与预设数据文件不相同，则初始数据文件与预设数据文件分别计算得到的哈希值也不相同。

[0096] 本实施例中，通过将文件保存到区块链中，并通过哈希值的数值比较，实现了文件的存证、取证和篡改验证。

[0097] 可选的，在上一个数据签名、加密及保存的方法的实施例的基础上，步骤S32可以包括：

[0098] 使用所述密钥信息中的私钥信息，对所述目标文件进行签名验证操作；

[0099] 若签名验证操作成功，使用所述密钥信息中的公钥信息，对进行签名验证操作后的目标文件进行解密操作，得到所述初始数据文件。

[0100] 具体的，签名验证和签名的过程互逆，加密过程和解密过程互逆。

[0101] 本实施例中，通过对目标文件进行签名验证和解密操作，从目标文件中提取得到初始数据文件。

[0102] 可选的，在上述应用于第一电子设备的数据签名、加密及保存的方法的实施例的基础上，本发明的另一实施例提供了一种数据签名、加密及保存的装置，应用于第一电子设备，参照图4，可以包括：

[0103] 数据验证模块101，用于获取用户的身份验证信息，并对所述身份验证信息进行验证；

[0104] 请求发送模块102，用于若验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息；所述密码获取请求包括所述身份信息；

[0105] 数据处理模块103，用于使用所述密钥信息对预设数据文件进行签名加密操作，得到目标文件，并将所述目标文件发送至第二电子设备；

[0106] 数据保存模块104，用于将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证。

[0107] 进一步，所述数据处理模块包括：

[0108] 第一处理子模块，用于使用所述密钥信息中的公钥信息，对预设数据文件进行加密操作；

[0109] 第二处理子模块，用于使用所述密钥信息中的私钥信息，对进行加密操作后的预设数据文件进行签名操作。

[0110] 本发明实施例中，数据文件保存在区块链中，区块链本身具有数据防篡改功能，进而能够提高数据安全性。

[0111] 另外，基于区块链技术和SM9算法来实现电子合同的签署、重要文件的存证取证。SM9算法可以实现数据的真实性、完整性、私密性、不可抵赖性。区块链技术可实现操作的全网、全过程、全交易的数据记录，其记录不可篡改。所有数据被全网所有节点共同拥有，网络空间的信息更加透明、行为更加可追溯，从而实现完整合规的合同签署过程。本实施例中，利用密码算法实现用户身份认证，并将用户签名行为、合同签署，通过区块链的分布式节点，建立人、事件、时间、地点等签名行为的溯源，签名行为、重要文件摘要特征值全链公开、可监督、可追溯，利用区块链技术的防篡改和防抵赖，实现可靠电子签名。并在身份可信的

基础上，进一步支撑区块链上各业务的真实、可信，为业务提供可信区块链技术服务。

[0112] 需要说明的是，本实施例中的各个模块和子模块的工作过程，请参照上述实施例中的相应说明，在此不再赘述。

[0113] 可选的，在上述应用于第二电子设备的数据签名、加密及保存的方法的实施例的基础上，本发明的另一实施例提供了一种数据签名、加密及保存的装置，应用于第二电子设备，参照图5，可以包括：

[0114] 数据获取模块101，用于接收第一电子设备发送的目标文件、获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件；

[0115] 文件确定模块102，用于根据所述密钥信息，从所述目标文件中确定初始数据文件；

[0116] 计算模块103，用于计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值；

[0117] 结果确定模块104，用于依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

[0118] 进一步，所述文件确定模块包括：

[0119] 第三处理子模块，用于使用所述密钥信息中的私钥信息，对所述目标文件进行签名验证操作；

[0120] 第四处理子模块，用于若签名验证操作成功，使用所述密钥信息中的公钥信息，对进行签名验证操作后的目标文件进行解密操作，得到所述初始数据文件。

[0121] 进一步，所述结果确定模块包括：

[0122] 第一确定子模块，用于若所述第一哈希值与所述第二哈希值相同，则确定所述目标文件未被篡改；

[0123] 第二确定子模块，用于若所述第一哈希值与所述第二哈希值不相同，则确定所述目标文件被篡改。

[0124] 本实施例中，通过将文件保存到区块链中，并通过哈希值的数值比较，实现了文件的存证、取证和篡改验证。

[0125] 需要说明的是，本实施例中的各个模块和子模块的工作过程，请参照上述实施例中的相应说明，在此不再赘述。

[0126] 可选的，在上述应用于第一电子设备的数据签名、加密及保存的方法及装置的实施例的基础上，本发明另一实施例提供了一种电子设备，包括：处理器和发送端口；

[0127] 其中，所述处理器，用于获取用户的身份验证信息，并对所述身份验证信息进行验证，使用密钥信息对预设数据文件进行签名加密操作，得到目标文件，将所述预设数据文件保存到区块链中，以使所述第二电子设备在获取到所述目标文件后，依据所述区块链中保存的所述预设数据对接收到的目标文件进行篡改验证；

[0128] 所述发送端口，用于若所述处理器对身份验证信息验证通过，发送密码获取请求至预设密码处理设备，以获取与所述身份验证信息中的身份信息相对应的密钥信息，并将所述目标文件发送至第二电子设备；所述密码获取请求包括所述身份信息。

[0129] 本发明实施例中，数据文件保存在区块链中，区块链本身具有数据防篡改功能，进

而能够提高数据安全性。

[0130] 另外，基于区块链技术和SM9算法来实现电子合同的签署、重要文件的存证取证。SM9算法可以实现数据的真实性、完整性、私密性、不可抵赖性。区块链技术可实现操作的全网、全过程、全交易的数据记录，其记录不可篡改。所有数据被全网所有节点共同拥有，网络空间的信息更加透明、行为更加可追溯，从而实现完整合规的合同签署过程。本实施例中，利用密码算法实现用户身份认证，并将用户签名行为、合同签署，通过区块链的分布式节点，建立人、事件、时间、地点等签名行为的溯源，签名行为、重要文件摘要特征值全链公开、可监督、可追溯，利用区块链技术的防篡改和防抵赖，实现可靠电子签名。并在身份可信的基础上，进一步支撑区块链上各业务的真实、可信，为业务提供可信区块链技术服务。

[0131] 可选的，在上述应用于第二电子设备的数据签名、加密及保存的方法及装置的实施例的基础上，本发明另一实施例提供了一种电子设备，包括：处理器和接收端口；

[0132] 所述接收端口，用于接收第一电子设备发送的目标文件；

[0133] 所述处理器，用于获取预设密码处理设备发送给所述第一电子设备的密钥信息，以及从区块链中获取所述第一电子设备保存的预设数据文件，根据所述密钥信息，从所述目标文件中确定初始数据文件，计算所述预设数据文件的第一哈希值和所述初始数据文件的第二哈希值，依据所述第一哈希值与所述第二哈希值是否相同的比较结果，确定所述第一电子设备发送的目标文件是否被篡改的结果。

[0134] 本实施例中，通过将文件保存到区块链中，并通过哈希值的数值比较，实现了文件的存证、取证和篡改验证。

[0135] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

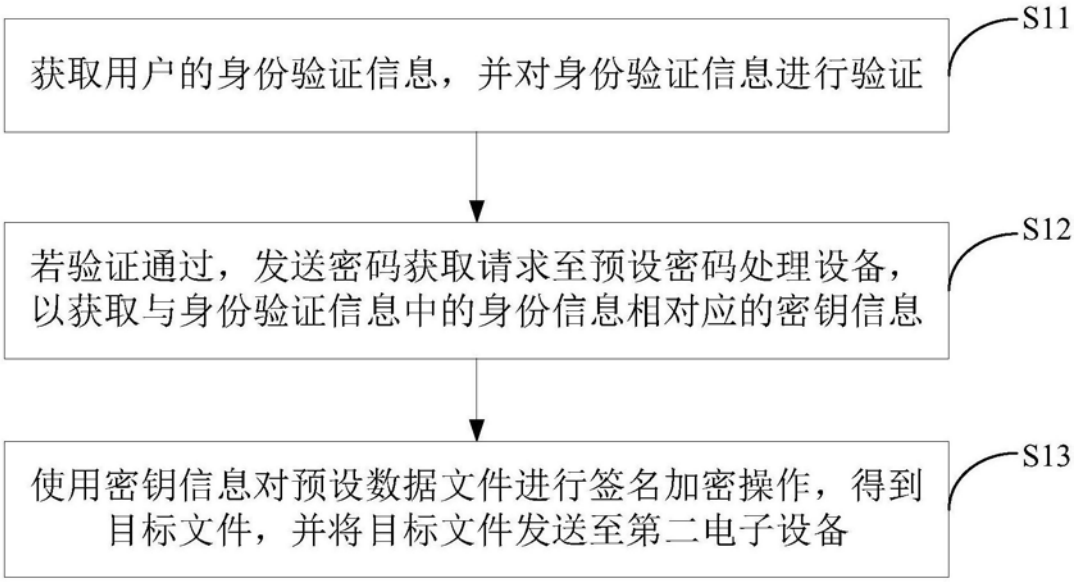

S11
获取用户的身份验证信息，并对身份验证信息进行验证
S12
若验证通过，发送密码获取请求至预设密码处理设备，以获取与身份验证信息中的身份信息相对应的密钥信息
S13
使用密钥信息对预设数据文件进行签名加密操作，得到目标文件，并将目标文件发送至第二电子设备

图1

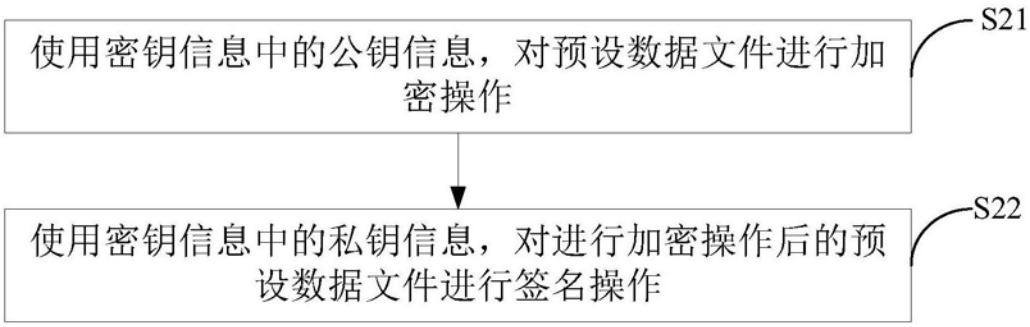

S21
使用密钥信息中的公钥信息，对预设数据文件进行加密操作
S22
使用密钥信息中的私钥信息，对进行加密操作后的预设数据文件进行签名操作

图2

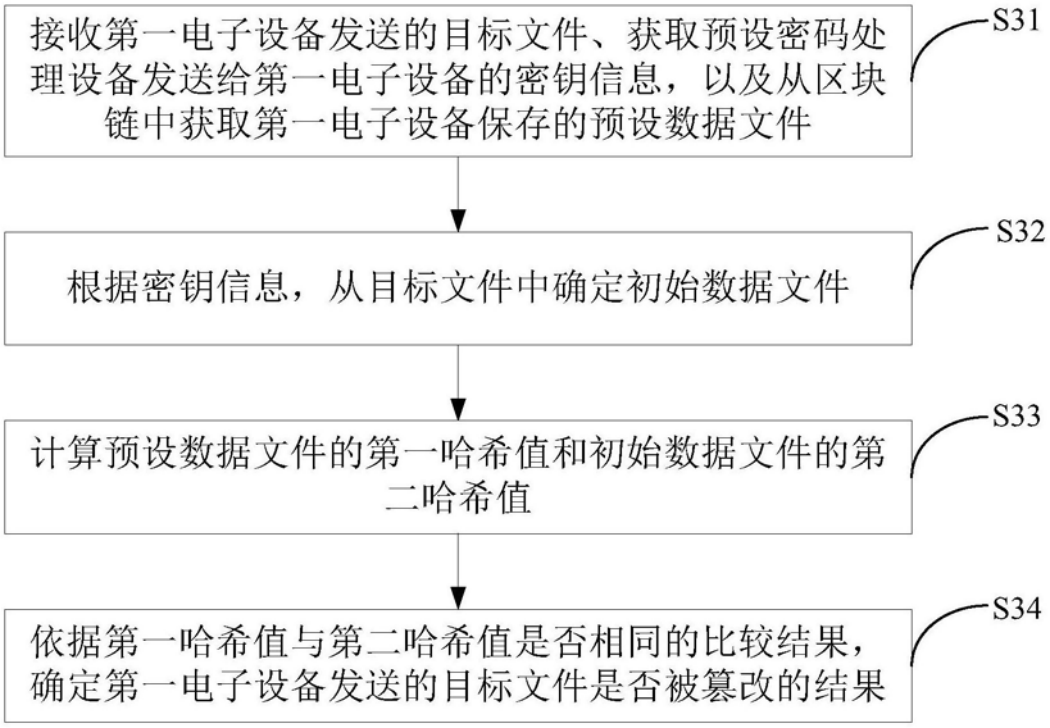

接收第一电子设备发送的目标文件、获取预设密码处理设备发送给第一电子设备的密钥信息，以及从区块链中获取第一电子设备保存的预设数据文件
S31
根据密钥信息，从目标文件中确定初始数据文件
S32
计算预设数据文件的第一哈希值和初始数据文件的第二哈希值
S33
依据第一哈希值与第二哈希值是否相同的比较结果，确定第一电子设备发送的目标文件是否被篡改的结果
S34

图3


101
数据验证模块
102
请求发送模块
103
数据处理模块
104
数据保存模块

图4

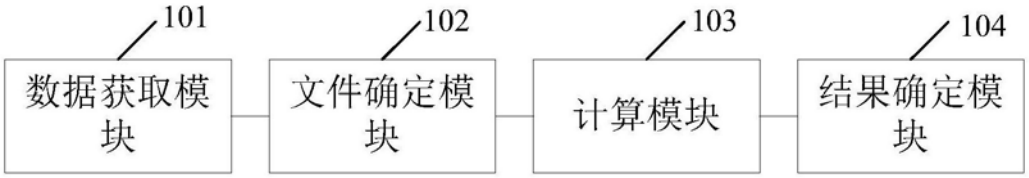

101
数据获取模块
102
文件确定模块
103
计算模块
104
结果确定模块

图5