(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112507391 B
(45)授权公告日 2024.01.30

(21)申请号 202011398822.1

(22)申请日 2020.12.01

(65)同一申请的已公布的文献号
申请公布号 CN 112507391 A

(43)申请公布日 2021.03.16

(73)专利权人 杭州企达信息技术有限公司
地址 310000 浙江省杭州市滨江区西兴街道锦绣玲珑府1幢712室

(72)发明人 柯宗甫 杨明军

(74)专利代理机构 杭州五洲普华专利代理事务所(特殊普通合伙) 33260
专利代理师 徐晶晶

(51)Int.Cl.
*G06F 21/64*(2013.01)
*G06F 21/31*(2013.01)
*G06F 21/60*(2013.01)

(56)对比文件
CN 109472166 A,2019.03.15
CN 110826092 A,2020.02.21
CN 111859431 A,2020.10.30
CN 108737430 A,2018.11.02
CN 110826091 A,2020.02.21
CN 111295869 A,2020.06.16
CN 110798315 A,2020.02.14
CN 110830256 A,2020.02.21
CN 111935075 A,2020.11.13
CN 108768630 A,2018.11.06
US 2020202345 A1,2020.06.25
艾孜买提·艾克木江.对等网络环境下的多方协作区块链公文签章应用研究.《电脑知识与技术》.2020,第16卷(第05期),29-30.
马舒婕.基于区块链的存储结构的设计与实现.《中国优秀硕士学位论文全文数据库 信息科技辑》.2020,(第06期),I137-67.

审查员 周杨

权利要求书3页 说明书10页 附图1页

(54)发明名称

基于区块链的电子签章方法、系统、装置及可读存储介质

(57)摘要

本发明公开一种基于区块链的电子签章方法,包括:响应于第一用户发送的电子签章请求,基于待签章文件标识获取待签章文件并加密存证于区块链网络节点中;根据所述电子签章请求查询并确定对应的区块链智能合约第一用户标识样本库和区块链智能合约待签章文件标识样本库;对第一用户进行身份验证,及对待签章文件进行文件合理性验证,两者都验证通过后,则将验证结果存证于区块链网络节点中;获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章,并将所述电子签名发布至区块链网络节点中进行存证。对请求签章的人和文件以及签章人采用区块链技术进行多重验证,这样能更有效的防止数据被修改,从根本上阻止电子签章的造假。


CN 112507391 B

1.一种基于区块链的电子签章方法,其特征在于,包括以下步骤:

响应于第一用户发送的电子签章请求,对所述请求进行解析,获取所述请求携带的第一用户标识、待签章文件标识及密钥数据,其中,电子签章请求中包含第一用户标识、待签章文件标识和密钥数据,所述密钥数据包括公钥和私钥;

基于待签章文件标识获取待签章文件,基于公钥对所述待签章文件进行加密,得到待签章加密文件并存证于区块链网络节点中;

根据所述电子签章请求查询并确定对应的区块链智能合约第一用户标识样本库和区块链智能合约待签章文件标识样本库;

调用区块链智能合约第一用户标识样本库和待签章文件标识样本库,根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,两者都验证通过后,则将验证结果存证于区块链网络节点中;

将验证结果发送至电子签名客户端,以使所述电子签名客户端对验证结果进行响应;

获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章,并将所述电子签名发布至区块链网络节点中进行存证;

其中,还包括生成样本库的步骤:

采集所有合法第一用户的身份信息、所有签章文件的合理性条件信息和第一用户密钥数据,其中,第一用户密钥数据包括第一公钥和第一私钥;

基于第一公钥数据对第一用户的身份信息进行加密,得到加密身份信息并存证于区块链网络节点中;

基于所述加密身份信息,调用预先设置在区块链网络中的智能合约第一用户绑定服务基于身份信息匹配规则建立第一用户标识样本库;

基于所有签章文件的合理性条件信息,调用预先设置在区块链网络中的智能合约关键字搜索服务基于关键字相似度规则,生成待签章文件标识样本库;

其中,所述根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,具体步骤为:

基于身份信息匹配规则,在第一用户标识样本库中查找第一用户标识对应的加密身份信息;

通过第一私钥对加密身份信息进行解密,得到解密后的身份信息;

将第一用户标识和解密后的身份信息进行匹配,若成功,则通过验证;

其中,所述根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,具体步骤包括:

基于关键字相似度规则,在待签章文件标识样本库中查找与待签章文件内容接近的签章文件合理性条件信息;将待签章文件和签章文件合理性条件信息进行比对核实,若待签章文件符合签章文件合理性条件信息,则合理性验证通过。

2.根据权利要求1所述的基于区块链的电子签章方法,其特征在于,还包括对电子签章进行验证的步骤,具体包括:

获取签名用户的身份信息,与区块链网络中预设的合法签名用户身份信息样本进行验证,若验证通过,则电子签章为有效签章,其中,身份信息为生物识别信息,生物识别信息包

括指纹信息、虹膜信息和人脸信息中的一种或几种。

3.根据权利要求2所述的基于区块链的电子签章方法,其特征在于,还包括生成合法签名用户身份信息样本步骤:

获取所有合法签名用户身份信息和第二密钥数据,其中,所述第二密钥数据包括第二公钥和第二私钥,基于第二公钥将所述所有合法签名用户身份信息进行加密,得到所有加密合法签名用户身份信息样本并发布在区块链网络中。

4.根据权利要求3所述的基于区块链的电子签章方法,其特征在于,所述与区块链网络中预设的合法签名用户身份信息样本进行验证,具体步骤包括:

在合法签名用户身份信息样本中查找与签名用户身份相应的加密合法签名用户身份信息;

通过第二私钥对加密合法签名用户身份信息进行解密,得到解密后的签名用户身份信息;

将签名用户的身份信息和解密后的解密后的签名用户身份信息进行匹配,若成功,则通过验证。

5.一种基于区块链的电子签章系统,其特征在于,包括响应解析模块、第一加密存证模块、查询确定模块、匹配验证模块、发送相应模块和获取发布模块;

所述响应解析模块,用于响应于第一用户发送的电子签章请求,对所述请求进行解析,获取所述请求携带的第一用户标识、待签章文件标识及密钥数据,其中,电子签章请求中包含第一用户标识、待签章文件标识和密钥数据,所述密钥数据包括公钥和私钥;

所述第一加密存证模块,用于基于待签章文件标识获取待签章文件,基于公钥对所述待签章文件进行加密,得到待签章加密文件并存证于区块链网络节点中;

所述查询确定模块,用于根据所述电子签章请求查询并确定对应的第一用户标识样本库和待签章文件标识样本库;

所述匹配验证模块,用于调用区块链智能合约第一用户标识样本库和待签章文件标识样本库,根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,两者都验证通过后,则将验证结果存证于区块链网络节点中;

所述发送相应模块,用于将验证结果发送至电子签名客户端,以使所述电子签名客户端对验证结果进行响应;

所述获取发布模块,用于获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章,并将所述电子签名发布至区块链网络节点中进行存证;

其中,还包括生成样本库的步骤:

采集所有合法第一用户的身份信息、所有签章文件的合理性条件信息和第一用户密钥数据,其中,第一用户密钥数据包括第一公钥和第一私钥;

基于第一公钥数据对第一用户的身份信息进行加密,得到加密身份信息并存证于区块链网络节点中;

基于所述加密身份信息,调用预先设置在区块链网络中的智能合约第一用户绑定服务基于身份信息匹配规则建立第一用户标识样本库;

基于所有签章文件的合理性条件信息,调用预先设置在区块链网络中的智能合约关键

字搜索服务基于关键字相似度规则,生成待签章文件标识样本库;

其中,所述根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,具体步骤为:

基于身份信息匹配规则,在第一用户标识样本库中查找第一用户标识对应的加密身份信息;

通过第一私钥对加密身份信息进行解密,得到解密后的身份信息;

将第一用户标识和解密后的身份信息进行匹配,若成功,则通过验证;

其中,所述根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,具体步骤包括:

基于关键字相似度规则,在待签章文件标识样本库中查找与待签章文件内容接近的签章文件合理性条件信息;将待签章文件和签章文件合理性条件信息进行比对核实,若待签章文件符合签章文件合理性条件信息,则合理性验证通过。

6.一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现如权利要求1至4任意一项所述的方法。

7.一种基于区块链的电子签章装置,包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现如权利要求1至4任意一项所述的方法。

# 基于区块链的电子签章方法、系统、装置及可读存储介质

## 技术领域

[0001] 本发明涉及区块链技术领域,尤其涉及一种基于区块链的电子签章方法、系统、装置及可读存储介质。

## 背景技术

[0002] 现在技术中,随着科技的发展,电子签章以其签署电子文件不受时间、空间的限制而广受青睐,广泛应用于,电子政务、企业电子商务、金融机构信息安全、物流行业、医疗卫生行业信息化、军队战地指挥化等领域。电子签章系统不仅可以辨识电子文件签署者的身份,还能确保文件的真实性、完整性和不可抵赖性。

[0003] 当下大火的区块链技术,是一种由若干台计算设备共同参与“记账”,共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性,使得区块链技术已在众多的领域中广泛的进行应用,也和电子签章系统有了火花的碰撞,将区块链技术应用在了电子签章技术中,虽然两者都存在不可抵赖性,但是还存在一定的弊端。

[0004] 在对电子文件签章的过程中,由于申请数字证书的流程较为繁琐,所以签章效率低下,并且最重要的是根本无法确保电子文件和签章授权人或者签章人的身份,如果两者都是假冒的,那么势必会造成各种损失,后果很严重。

## 发明内容

[0005] 本发明针对现有技术中的缺点,提供了一种基于区块链的电子签章方法、系统、装置及可读存储介质。

[0006] 为了解决上述技术问题,本发明通过下述技术方案得以解决:

[0007] 一种基于区块链的电子签章方法,包括以下步骤:

[0008] 响应于第一用户发送的电子签章请求,对所述请求进行解析,获取所述请求携带的第一用户标识、待签章文件标识及密钥数据,其中,电子签章请求中包含第一用户标识、待签章文件标识和密钥数据,所述密钥数据包括公钥和私钥;

[0009] 基于待签章文件标识获取待签章文件,基于公钥对所述待签章文件进行加密,得到待签章加密文件并存证于区块链网络节点中;

[0010] 根据所述电子签章请求查询并确定对应的区块链智能合约第一用户标识样本库和区块链智能合约待签章文件标识样本库;

[0011] 调用区块链智能合约第一用户标识样本库和待签章文件标识样本库,根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,两者都验证通过后,则将验证结果存证于区块链网络节点中;

[0012] 将验证结果发送至电子签名客户端,以使所述电子签名客户端对验证结果进行响应;

[0013] 获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章,并将所述电子签名发布至区块链网络节点中进行存证。

[0014] 作为一种可实施方式,还包括生成样本库的步骤:

[0015] 采集所有合法第一用户的身份信息、所有签章文件的合理性条件信息和第一用户密钥数据,其中,第一用户密钥数据包括第一公钥和第一私钥;

[0016] 基于第一公钥数据对第一用户的身份信息进行加密,得到加密身份信息并存证于区块链网络节点中;

[0017] 基于所述加密身份信息,调用预先设置在区块链网络中的智能合约第一用户绑定服务基于身份信息匹配规则建立第一用户标识样本库;

[0018] 基于所有签章文件的合理性条件信息,调用预先设置在区块链网络中的智能合约关键字搜索服务基于关键字相似度规则,生成待签章文件标识样本库。

[0019] 作为一种可实施方式,所述根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,具体步骤为:

[0020] 基于身份信息匹配规则,在第一用户标识样本库中查找第一用户标识对应的加密身份信息;

[0021] 通过第一私钥对加密身份信息进行解密,得到解密后的身份信息;

[0022] 将第一用户标识和解密后的身份信息进行匹配,若成功,则通过验证。

[0023] 作为一种可实施方式,所述根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,具体步骤包括:

[0024] 基于关键字相似度规则,在签章文件标识样本库中查找与待签章文件内容接近的签章文件合理性条件信息;将待签章文件和签章文件合理性条件信息进行比对核实,若待签章文件符合签章文件合理性条件信息,则合理性验证通过。

[0025] 作为一种可实施方式,还包括对电子签章进行验证的步骤,具体包括:

[0026] 获取签名用户的身份信息,与区块链网络中预设的合法签名用户身份信息样本进行验证,若验证通过,则电子签章为有效签章,其中,身份信息为生物识别信息,生物识别信息包括指纹信息、虹膜信息和人脸信息中的一种或几种。

[0027] 作为一种可实施方式,还包括生成合法签名用户身份信息样本步骤:

[0028] 获取所有合法签名用户身份信息和第二密钥数据,其中,所述第二密钥数据包括第二公钥和第二私钥,基于第二公钥将所述所有合法签名用户身份信息进行加密,得到所有加密合法签名用户身份信息样本并发布在区块链网络中。

[0029] 作为一种可实施方式,所述与区块链网络中预设的合法签名用户身份信息样本进行验证,具体步骤包括:

[0030] 在合法签名用户身份信息样本中查找与签名用户身份相应的加密合法签名用户身份信息;

[0031] 通过第二私钥对加密合法签名用户身份信息进行解密,得到解密后的签名用户身份信息;

[0032] 将签名用户的身份信息和解密后的解密后的签名用户身份信息进行匹配,若成功,则通过验证。

[0033] 一种基于区块链的电子签章系统,包括响应解析模块、第一加密存证模块、查询确

定模块、匹配验证模块、发送相应模块和获取发布模块；

[0034] 所述响应解析模块，用于响应于第一用户发送的电子签章请求，对所述请求进行解析，获取所述请求携带的第一用户标识、待签章文件标识及密钥数据，其中，电子签章请求中包含第一用户标识、待签章文件标识和密钥数据，所述密钥数据包括公钥和私钥；

[0035] 所述第一加密存证模块，用于基于待签章文件标识获取待签章文件，基于公钥对所述待签章文件进行加密，得到待签章加密文件并存证于区块链网络节点中；

[0036] 所述查询确定模块，用于根据所述电子签章请求查询并确定对应的第一用户标识样本库和待签章文件标识样本库；

[0037] 所述匹配验证模块，用于调用区块链智能合约第一用户标识样本库和待签章文件标识样本库，根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证，及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证，两者都验证通过后，则将验证结果存证于区块链网络节点中；

[0038] 所述发送相应模块，用于将验证结果发送至电子签名客户端，以使所述电子签名客户端对验证结果进行响应；

[0039] 所述获取发布模块，用于获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章，并将所述电子签名发布至区块链网络节点中进行存证。

[0040] 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现如下的方法步骤：

[0041] 响应于第一用户发送的电子签章请求，对所述请求进行解析，获取所述请求携带的第一用户标识、待签章文件标识及密钥数据，其中，电子签章请求中包含第一用户标识、待签章文件标识和密钥数据，所述密钥数据包括公钥和私钥；

[0042] 基于待签章文件标识获取待签章文件，基于公钥对所述待签章文件进行加密，得到待签章加密文件并存证于区块链网络节点中；

[0043] 根据所述电子签章请求查询并确定对应的区块链智能合约第一用户标识样本库和区块链智能合约待签章文件标识样本库；

[0044] 调用区块链智能合约第一用户标识样本库和待签章文件标识样本库，根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证，及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证，两者都验证通过后，则将验证结果存证于区块链网络节点中；

[0045] 将验证结果发送至电子签名客户端，以使所述电子签名客户端对验证结果进行响应；

[0046] 获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章，并将所述电子签名发布至区块链网络节点中进行存证。

[0047] 一种基于区块链的电子签章装置，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如下的方法步骤：

[0048] 响应于第一用户发送的电子签章请求，对所述请求进行解析，获取所述请求携带的第一用户标识、待签章文件标识及密钥数据，其中，电子签章请求中包含第一用户标识、待签章文件标识和密钥数据，所述密钥数据包括公钥和私钥；

[0049] 基于待签章文件标识获取待签章文件,基于公钥对所述待签章文件进行加密,得到待签章加密文件并存证于区块链网络节点中;

[0050] 根据所述电子签章请求查询并确定对应的区块链智能合约第一用户标识样本库和区块链智能合约待签章文件标识样本库;

[0051] 调用区块链智能合约第一用户标识样本库和待签章文件标识样本库,根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,两者都验证通过后,则将验证结果存证于区块链网络节点中;

[0052] 将验证结果发送至电子签名客户端,以使所述电子签名客户端对验证结果进行响应;

[0053] 获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章,并将所述电子签名发布至区块链网络节点中进行存证。

[0054] 本发明由于采用了以上技术方案,具有显著的技术效果:

[0055] 通过本发明的方法,对请求签章的人和文件以及签章人采用区块链技术进行多重验证,在验证的过程中为了保证数据不被篡改和丢失,还采用了加密解密技术,这样能更有效的防止数据被修改,从根本上阻止电子签章的造假。

## 附图说明

[0056] 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一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0057] 图1是本发明方法的整体流程示意图;

[0058] 图2是本发明系统的整体结构示意图。

## 具体实施方式

[0059] 下面结合实施例对本发明做进一步的详细说明,以下实施例是对本发明的解释而本发明并不局限于以下实施例。

[0060] 现在技术中,随着科技的发展,电子签章以其签署电子文件不受时间、空间的限制而广受青睐,广泛应用于,电子政务、企业电子商务、金融机构信息安全、物流行业、医疗卫生行业信息化、军队战地指挥化等领域。电子签章系统不仅可以辨识电子文件签署者的身份,还能确保文件的真实性、完整性和不可抵赖性。

[0061] 当下大火的区块链技术,是一种由若干台计算设备共同参与“记账”,共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性,使得区块链技术已在众多的领域中广泛的进行应用,也和电子签章系统有了火花的碰撞,将区块链技术应用在了电子签章技术中,虽然两者都存在不可抵赖性,但是还存在一定的弊端。

[0062] 在对电子文件签章的过程中,由于申请数字证书的流程较为繁琐,所以签章效率低下,并且最重要的是根本无法确保电子文件和签章授权人或者签章人的身份,如果两者

都是假冒的,那么势必会造成各种损失,后果很严重。

[0063] 实施例1:

[0064] 一种基于区块链的电子签章方法,如图1所示,包括以下步骤:

[0065] S100、响应于第一用户发送的电子签章请求,对所述请求进行解析,获取所述请求携带的第一用户标识、待签章文件标识及密钥数据,其中,电子签章请求中包含第一用户标识、待签章文件标识和密钥数据,所述密钥数据包括公钥和私钥;

[0066] S200、基于待签章文件标识获取待签章文件,基于公钥对所述待签章文件进行加密,得到待签章加密文件并存证于区块链网络节点中;

[0067] S300、根据所述电子签章请求查询并确定对应的区块链智能合约第一用户标识样本库和区块链智能合约待签章文件标识样本库;

[0068] S400、调用区块链智能合约第一用户标识样本库和待签章文件标识样本库,根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,两者都验证通过后,则将验证结果存证于区块链网络节点中;

[0069] S500、将验证结果发送至电子签名客户端,以使所述电子签名客户端对验证结果进行响应;

[0070] S600、获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章,并将所述电子签名发布至区块链网络节点中进行存证。

[0071] 在IM消息发送过程中或者其他场景下,假设通过网络给一份文件或者其他待签文件请求电子签章或者电子签名,很难识别请求者或者待签文件是否有问题,比如,可能是不法份子冒充同事或者签章请求者请求签章或者签名,或者是有不法文件传一份非正常合同进行签章,假如不进行验证,那么签名用户或者签章用户会直接进行进行签章;亦或者是请求签章的人和文件是正常的,但是签名用户或者签章用户有问题,这样都会使得电子签章有问题,可能会给公司或者个人造成极大的损失。

[0072] 通过本发明的方法,当接收到电子签章请求时,会同时获取到第一用户标识、待签章文件标识及密钥数据,先对待签章文件进行加密并且存证,先把待签章文件加密是为了保证数据安全以及后续的取证,再去验证第一用户和待签章文件是否合理,两者都验证通过后才可以进行电子签章,本发明对请求签章的人和文件采用区块链技术进行多重验证,在验证的过程中为了保证数据不被篡改和丢失,还采用了加密解密技术,这样能更有效的防止数据被修改,从根本上阻止电子签章的造假。

[0073] 在一个实施例中,还包括生成样本库的步骤:

[0074] 采集所有合法第一用户的身份信息、所有签章文件的合理性条件信息和第一用户密钥数据,其中,第一用户密钥数据包括第一公钥和第一私钥;

[0075] 基于第一公钥数据对第一用户的身份信息进行加密,得到加密身份信息并存证于区块链网络节点中;

[0076] 基于所述加密身份信息,调用预先设置在区块链网络中的智能合约第一用户绑定服务基于身份信息匹配规则建立第一用户标识样本库;

[0077] 基于所有签章文件的合理性条件信息,调用预先设置在区块链网络中的智能合约关键字搜索服务基于关键字相似度规则,生成待签章文件标识样本库。

[0078] 此实施例是生成样本库的具体步骤,在生成样本库的过程中,为了保证数据不被轻易的破解,采用了加密解密的技术,这样能保证数据的安全;

[0079] 第一用户标识包含了第一用户特有的身份信息,比如指纹、脸部图像、眼睛等,将这些特有的身份信息存放在第一用户标识样本库中,就是为了后续验证第一用户是否为合法用户;

[0080] 另外,为了防止不法分子窃取电子签章,还要对待签章文件进行核实,因此建立了待签章文件标识样本库,比如记载了哪些文件或者哪些情况下,待签章文件验证不通过;可以采用现有方式训练出不合理条件筛选模型,比如,采集很有很多不合理条件的图片进行训练,形成不合理条件筛选模型,亦或者采集很多不合理条件的文字进行训练,形成不合理条件筛选的文本表示模型等,通过这些模型对待签章文件进行核实,如果出现不合理的文字或者条款,则需要人工进一步对待签章文件进行审核,以确保待签章文件的合理性。

[0081] 于其他实施例中,所述根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,具体步骤为:

[0082] 基于身份信息匹配规则,在第一用户标识样本库中查找第一用户标识对应的加密身份信息;

[0083] 通过第一私钥对加密身份信息进行解密,得到解密后的身份信息;

[0084] 将第一用户标识和解密后的身份信息进行匹配,若成功,则通过验证。

[0085] 在此实施例中,由于建立第一用户标识样本库时其中的身份信息已经被加密,因此,在验证时需要进行解密,这样数据才够安全。在一个实施例中,所述根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,具体步骤包括:

[0086] 基于关键字相似度规则,在签章文件标识样本库中查找与待签章文件内容接近的签章文件合理性条件信息;将待签章文件和签章文件合理性条件信息进行比对核实,若待签章文件符合签章文件合理性条件信息,则合理性验证通过。

[0087] 为了能保证签章用户的电子签章是合法并非伪造的,因此需要对签章用户进行验证,还包括对电子签章进行验证的步骤,具体包括:

[0088] 获取签名用户的身份信息,与区块链网络中预设的合法签名用户身份信息样本进行验证,若验证通过,则电子签章为有效签章,其中,身份信息为生物识别信息,生物识别信息包括指纹信息、虹膜信息和人脸信息中的一种或几种。

[0089] 为了能够更加顺利的进行签名用户合法化的验证,此实施例详细的讲述了生成合法签名用户身份信息样本步骤:

[0090] 获取所有合法签名用户身份信息和第二密钥数据,其中,所述第二密钥数据包括第二公钥和第二私钥,基于第二公钥将所述所有合法签名用户身份信息进行加密,得到所有加密合法签名用户身份信息样本并发布在区块链网络中。

[0091] 基于以上实施例中生成的合法签名用户身份信息样本,所述与区块链网络中预设的合法签名用户身份信息样本进行验证,具体步骤包括:

[0092] 在合法签名用户身份信息样本中查找与签名用户身份相应的加密合法签名用户身份信息;

[0093] 通过第二私钥对加密合法签名用户身份信息进行解密,得到解密后的签名用户身

份信息；

[0094] 将签名用户的身份信息和解密后的解密后的签名用户身份信息进行匹配，若成功，则通过验证。

[0095] 也就是说：不仅第一用户(即请求签章人员)会造假，在签章的过程中，可能签名用户也会造假，比如冒充签章人员，因此，也要验证签名用户，验证成功后才允许电子签章上链发布。

[0096] 实施例2：

[0097] 一种基于区块链的电子签章系统，如图2所示，包括响应解析模块100、第一加密存证模块200、查询确定模块300、匹配验证模块400、发送相应模块500和获取发布模块600；

[0098] 所述响应解析模块100，用于响应于第一用户发送的电子签章请求，对所述请求进行解析，获取所述请求携带的第一用户标识、待签章文件标识及密钥数据，其中，电子签章请求中包含第一用户标识、待签章文件标识和密钥数据，所述密钥数据包括公钥和私钥；

[0099] 所述第一加密存证模块200，用于基于待签章文件标识获取待签章文件，基于公钥对所述待签章文件进行加密，得到待签章加密文件并存证于区块链网络节点中；

[0100] 所述查询确定模块300，用于根据所述电子签章请求查询并确定对应的第一用户标识样本库和待签章文件标识样本库；

[0101] 所述匹配验证模块400，用于调用区块链智能合约第一用户标识样本库和待签章文件标识样本库，根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证，及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证，两者都验证通过后，则将验证结果存证于区块链网络节点中；

[0102] 所述发送相应模块500，用于将验证结果发送至电子签名客户端，以使所述电子签名客户端对验证结果进行响应；

[0103] 所述获取发布模块600，用于获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章，并将所述电子签名发布至区块链网络节点中进行存证。

[0104] 在一个实施例中，所述查询确定模块300，被设置为：

[0105] 采集所有合法第一用户的身份信息、所有签章文件的合理性条件信息和第一用户密钥数据，其中，第一用户密钥数据包括第一公钥和第一私钥；

[0106] 基于第一公钥数据对第一用户的身份信息进行加密，得到加密身份信息并存证于区块链网络节点中；

[0107] 基于所述加密身份信息，调用预先设置在区块链网络中的智能合约第一用户绑定服务基于身份信息匹配规则建立第一用户标识样本库；

[0108] 基于所有签章文件的合理性条件信息，调用预先设置在区块链网络中的智能合约关键字搜索服务基于关键字相似度规则，生成待签章文件标识样本库。

[0109] 在一个实施例中，所述匹配验证模块400，被设置为：

[0110] 基于身份信息匹配规则，在第一用户标识样本库中查找第一用户标识对应的加密身份信息；

[0111] 通过第一私钥对加密身份信息进行解密，得到解密后的身份信息；

[0112] 将第一用户标识和解密后的身份信息进行匹配，若成功，则通过验证。

[0113] 在一个实施例中，所述匹配验证模块400，被设置为：

[0114] 基于关键字相似度规则,在签章文件标识样本库中查找与待签章文件内容接近的签章文件合理性条件信息;将待签章文件和签章文件合理性条件信息进行比对核实,若待签章文件符合签章文件合理性条件信息,则合理性验证通过。

[0115] 在一个实施例中,所述所述获取发布模块600,被设置为:

[0116] 获取签名用户的身份信息,与区块链网络中预设的合法签名用户身份信息样本进行验证,若验证通过,则电子签章为有效签章,其中,身份信息为生物识别信息,生物识别信息包括指纹信息、虹膜信息和人脸信息中的一种或几种。

[0117] 在一个实施例中,所述所述获取发布模块600,被设置为:

[0118] 获取所有合法签名用户身份信息和第二密钥数据,其中,所述第二密钥数据包括第二公钥和第二私钥,基于第二公钥将所述所有合法签名用户身份信息进行加密,得到所有加密合法签名用户身份信息样本并发布在区块链网络中。

[0119] 在一个实施例中,所述所述获取发布模块600,被设置为:

[0120] 在合法签名用户身份信息样本中查找与签名用户身份相应的加密合法签名用户身份信息;

[0121] 通过第二私钥对加密合法签名用户身份信息进行解密,得到解密后的签名用户身份信息;

[0122] 将签名用户的身份信息和解密后的解密后的签名用户身份信息进行匹配,若成功,则通过验证。

[0123] 实施例3:

[0124] 一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序被处理器执行时实现如下的方法步骤:

[0125] 响应于第一用户发送的电子签章请求,对所述请求进行解析,获取所述请求携带的第一用户标识、待签章文件标识及密钥数据,其中,电子签章请求中包含第一用户标识、待签章文件标识和密钥数据,所述密钥数据包括公钥和私钥;

[0126] 基于待签章文件标识获取待签章文件,基于公钥对所述待签章文件进行加密,得到待签章加密文件并存证于区块链网络节点中;

[0127] 根据所述电子签章请求查询并确定对应的区块链智能合约第一用户标识样本库和区块链智能合约待签章文件标识样本库;

[0128] 调用区块链智能合约第一用户标识样本库和待签章文件标识样本库,根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,两者都验证通过后,则将验证结果存证于区块链网络节点中;

[0129] 将验证结果发送至电子签名客户端,以使所述电子签名客户端对验证结果进行响应;

[0130] 获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章,并将所述电子签名发布至区块链网络节点中进行存证。

[0131] 在一个实施例中,处理器执行计算机程序时,实现还包括生成样本库的步骤:

[0132] 采集所有合法第一用户的身份信息、所有签章文件的合理性条件信息和第一用户密钥数据,其中,第一用户密钥数据包括第一公钥和第一私钥;

[0133] 基于第一公钥数据对第一用户的身份信息进行加密,得到加密身份信息并存证于区块链网络节点中;

[0134] 基于所述加密身份信息,调用预先设置在区块链网络中的智能合约第一用户绑定服务基于身份信息匹配规则建立第一用户标识样本库;

[0135] 基于所有签章文件的合理性条件信息,调用预先设置在区块链网络中的智能合约关键字搜索服务基于关键字相似度规则,生成待签章文件标识样本库。

[0136] 在一个实施例中,处理器执行计算机程序时,实现所述根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证,具体步骤为:

[0137] 基于身份信息匹配规则,在第一用户标识样本库中查找第一用户标识对应的加密身份信息;

[0138] 通过第一私钥对加密身份信息进行解密,得到解密后的身份信息;

[0139] 将第一用户标识和解密后的身份信息进行匹配,若成功,则通过验证。

[0140] 在一个实施例中,处理器执行计算机程序时,实现所述根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证,具体步骤包括:

[0141] 基于关键字相似度规则,在签章文件标识样本库中查找与待签章文件内容接近的签章文件合理性条件信息;将待签章文件和签章文件合理性条件信息进行比对核实,若待签章文件符合签章文件合理性条件信息,则合理性验证通过。

[0142] 在一个实施例中,处理器执行计算机程序时,实现还包括对电子签章进行验证的步骤,具体包括:

[0143] 获取签名用户的身份信息,与区块链网络中预设的合法签名用户身份信息样本进行验证,若验证通过,则电子签章为有效签章,其中,身份信息为生物识别信息,生物识别信息包括指纹信息、虹膜信息和人脸信息中的一种或几种。

[0144] 在一个实施例中,处理器执行计算机程序时,实现还包括生成合法签名用户身份信息样本步骤:

[0145] 获取所有合法签名用户身份信息和第二密钥数据,其中,所述第二密钥数据包括第二公钥和第二私钥,基于第二公钥将所述所有合法签名用户身份信息进行加密,得到所有加密合法签名用户身份信息样本并发布在区块链网络中。

[0146] 在一个实施例中,处理器执行计算机程序时,实现所述与区块链网络中预设的合法签名用户身份信息样本进行验证,具体步骤包括:

[0147] 在合法签名用户身份信息样本中查找与签名用户身份相应的加密合法签名用户身份信息;

[0148] 通过第二私钥对加密合法签名用户身份信息进行解密,得到解密后的签名用户身份信息;

[0149] 将签名用户的身份信息和解密后的解密后的签名用户身份信息进行匹配,若成功,则通过验证。

[0150] 实施例4:

[0151] 在一个实施例中,提供了一种基于区块链的电子签章装置,该基于区块链的电子签章装置可以是服务器也可以是移动终端。该基于区块链的电子签章装置包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中,该基于区块链的电子签章装置的处理

器用于提供计算和控制能力。该基于区块链的电子签章装置的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该数据库存储基于区块链的电子签章装置的所有数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现基于区块链的电子签章的方法。

[0152] 本说明书中的各个实施例均采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似的部分互相参见即可。

[0153] 本领域内的技术人员应明白,本发明的实施例可提供为方法、装置、或计算机程序产品。因此,本发明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,本发明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。

[0154] 本发明是参照根据本发明的方法、终端设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0155] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0156] 这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上,使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0157] 需要说明的是:

[0158] 说明书中提到的“一个实施例”或“实施例”意指结合实施例描述的特定特征、结构或特性包括在本发明的至少一个实施例中。因此,说明书通篇各个地方出现的短语“一个实施例”或“实施例”并不一定均指同一个实施例。

[0159] 此外,需要说明的是,本说明书中所描述的具体实施例,其零、部件的形状、所取名称等可以不同。凡依本发明专利构思所述的构造、特征及原理所做的等效或简单变化,均包括于本发明专利的保护范围内。本发明所属技术领域的技术人员可以对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代,只要不偏离本发明的结构或者超越本权利要求书所定义的范围,均应属于本发明的保护范围。

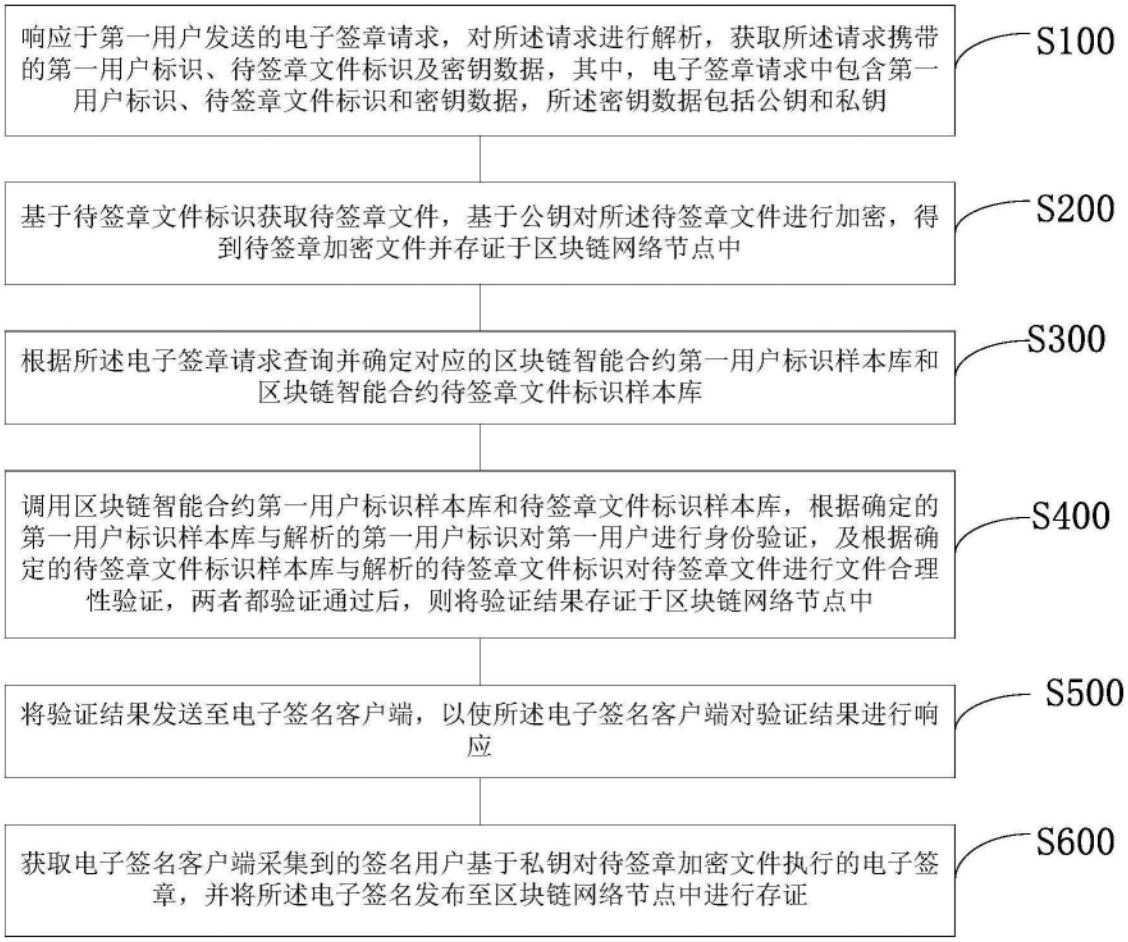
响应于第一用户发送的电子签章请求，对所述请求进行解析，获取所述请求携带的第一用户标识、待签章文件标识及密钥数据，其中，电子签章请求中包含第一用户标识、待签章文件标识和密钥数据，所述密钥数据包括公钥和私钥
S100
基于待签章文件标识获取待签章文件，基于公钥对所述待签章文件进行加密，得到待签章加密文件并存证于区块链网络节点中
S200
根据所述电子签章请求查询并确定对应的区块链智能合约第一用户标识样本库和区块链智能合约待签章文件标识样本库
S300
调用区块链智能合约第一用户标识样本库和待签章文件标识样本库，根据确定的第一用户标识样本库与解析的第一用户标识对第一用户进行身份验证，及根据确定的待签章文件标识样本库与解析的待签章文件标识对待签章文件进行文件合理性验证，两者都验证通过后，则将验证结果存证于区块链网络节点中
S400
将验证结果发送至电子签名客户端，以使所述电子签名客户端对验证结果进行响应
S500
获取电子签名客户端采集到的签名用户基于私钥对待签章加密文件执行的电子签章，并将所述电子签名发布至区块链网络节点中进行存证
S600

图1


响应解析模块
100
第一加密存证模块
200
查询确定模块
300
匹配验证模块
400
发送相应模块
500
获取发布模块
600

图2