



(12)发明专利申请

(10)申请公布号 CN 109508564 A

(43)申请公布日 2019. 03. 22

(21)申请号 201811563282.0

(22)申请日 2018.12.20

(71)申请人 姚前

地址 100055 北京市西城区鸭子桥路1号院
2号楼1806号

(72)发明人 姚前

(74)专利代理机构 中原信达知识产权代理有限
责任公司 11219

代理人 张一军 张效荣

(51)Int.Cl.

G06F 21/64(2013.01)

G06Q 30/00(2012.01)

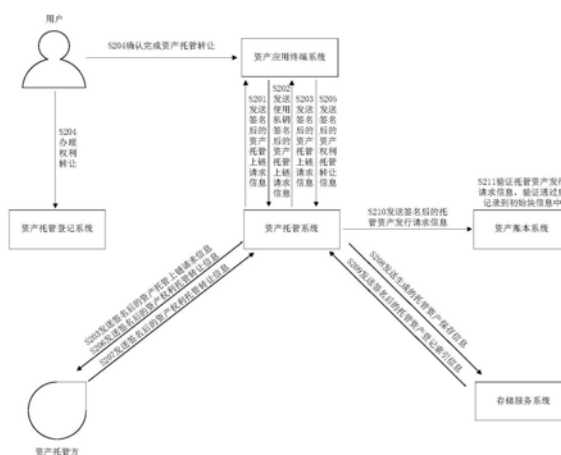
权利要求书3页 说明书11页 附图2页

(54)发明名称

一种基于区块链的数字资产存储系统和方法

(57)摘要

本发明公开了一种基于区块链的数字资产存储系统和方法,涉及数字资产技术领域。该系统的一具体实施方式包括:资产托管系统生成托管资产保存信息并发送至存储服务系统;存储服务系统接收并存储托管资产保存信息,之后将带有存储服务系统签名的托管资产登记索引信息反馈至资产托管系统;资产托管系统向资产账本系统发送带有资产托管系统签名的托管资产发行请求信息;资产账本系统对托管资产发行请求信息进行验证,验证通过后,将托管资产发行请求信息记录包含资产权利人的资产账本地址的初始块信息中。该实施方式将托管资产保存信息保存到链下的存储系统,将托管资产登记索引信息保存到链上的资产账本系统,实现了链上信息的轻量化存储。



1. 一种基于区块链的数字资产存储系统,其特征在于,包括:资产托管系统、资产账本系统和存储服务系统;其中,

所述资产托管系统,用于接收带有资产应用终端系统签名的资产权利托管转让信息,以生成托管资产保存信息并发送至所述存储服务系统,其中,所述托管资产保存信息包括资产托管上链请求信息和所述资产权利托管转让信息,所述资产托管上链请求信息包括链下资产托管转让请求信息和托管资产发行信息;

所述存储服务系统,用于接收并存储所述托管资产保存信息,之后将带有所述存储服务系统签名的托管资产登记索引信息反馈至所述资产托管系统;其中,所述托管资产登记索引信息包括托管资产登记索引标识和所述托管资产保存信息的防篡改信息;

所述资产托管系统,还用于向所述资产账本系统发送带有所述资产托管系统签名的托管资产发行请求信息,其中,所述托管资产发行请求信息包括带有所述存储服务系统签名的托管资产登记索引信息和所述托管资产发行信息;

所述资产账本系统,用于对所述托管资产发行请求信息进行验证,验证通过后,将所述托管资产发行请求信息记录到包含资产权利人的资产账本地址的初始块信息中。

2. 根据权利要求1所述的系统,其特征在于,所述防篡改信息为:所述托管资产保存信息的数字指纹信息,或利用所述资产托管系统和所述存储服务系统对所述数字指纹信息进行签名后的信息。

3. 根据权利要求1所述的系统,其特征在于,所述资产托管系统还用于:

根据所述链下资产托管转让请求信息和所述托管资产发行信息,生成所述资产托管上链请求信息,之后将带有所述资产托管系统签名的资产托管上链请求信息发送至所述资产应用终端系统;

所述资产应用终端系统,用于使用身份证书对应的用户私钥对所述资产托管上链请求信息进行签名,之后反馈至所述资产托管系统。

4. 根据权利要求3所述的系统,其特征在于,所述资产托管系统还用于:

接收来自所述资产应用终端系统的带有所述资产应用终端系统签名的资产权利托管转让信息,添加所述资产托管系统的签名后发送至资产托管方;

接收来自所述资产托管方的带有所述资产托管方签名的资产权利托管转让信息;其中,所述资产权利托管转让信息包括资产权利转让凭证信息、所述资产托管方持有资产的凭证信息、更新的链下资产登记信息。

5. 根据权利要求4所述的系统,其特征在于,所述对所述托管资产发行请求信息进行验证,包括:

验证所述托管资产发行请求信息的签名,以及所述托管资产登记索引信息的签名;

验证通过后,根据所述托管资产登记索引信息的托管资产登记索引标识从所述存储服务系统中获取对应的托管资产保存信息;

验证所述托管资产保存信息的防篡改信息,所述托管资产权利转让信息的三方签名,以及所述托管资产上链请求信息的双签名;其中,所述三方签名为所述资产托管系统、所述资产托管方和所述资产应用终端系统的签名,所述双签名为所述资产托管系统和所述资产应用终端系统的签名;

验证所述托管资产发行信息的权利人地址,与所述链下资产托管转让请求信息的实名

账本记录中的资产账本地址是否一致。

6. 根据权利要求1至5的任一项所述的系统,其特征在於,当所述防篡改信息为对所述托管资产保存信息进行哈希运算得到的哈希值的情况下,所述资产托管系统,还用于:

根据所述托管资产登记索引信息的托管资产登记索引标识,从所述存储服务系统中获取对应的托管资产保存信息;

对获取的所述托管资产保存信息进行哈希运算得到第二哈希值,将所述第二哈希值与所述托管资产登记索引信息包含的防篡改信息进行比较;

根据比较结果判断所述托管资产保存信息是否被篡改。

7. 根据权利要求1至5的任一项所述的系统,其特征在於,当所述防篡改信息为对所述托管资产保存信息进行哈希运算得到哈希值后,使用所述资产托管系统和所述存储服务系统的私钥分别对所述哈希值进行签名得到的结果的情况下,所述资产托管系统,还用于:

根据所述托管资产登记索引信息的托管资产登记索引标识,从所述存储服务系统中获取对应的托管资产保存信息;

对获取的所述托管资产保存信息进行哈希运算得到第二哈希值,使用所述资产托管系统和所述存储服务系统的公钥分别与对应的私钥签名进行验证。

8. 根据权利要求1或2所述的系统,其特征在於,所述系统还包括:资产应用终端系统;其中,

所述资产应用终端系统,用于基于所述资产权利人选择和/或输入的查询要求以及所述资产权利人对应的资产账本地址,生成第一链上资产查询请求信息,之后将所述第一链上资产查询请求信息发送至所述资产账本系统;

所述资产账本系统,还用于根据所述第一链上资产查询请求信息的资产账本地址,查询与所述资产账本地址相对应的链上资产信息以及与所述链上资产信息的托管资产类别相对应的初始块信息,之后反馈至所述资产应用终端系统;

所述资产应用终端系统,还用于基于所述资产权利人选择的所述初始块信息对应的托管资产登记索引标识,生成第二链上资产查询请求信息,之后将所述第二链上资产查询请求信息发送至存储服务系统;

所述存储服务系统,还用于根据所述第二链上资产查询请求信息的托管资产登记索引标识,查询与所述托管资产登记索引标识相对应的托管资产保存信息,之后反馈至所述资产应用终端系统。

9. 一种基于区块链的数字资产存储方法,其特征在於,包括以下步骤:

资产托管系统接收带有资产应用终端系统签名的资产权利托管转让信息,以生成托管资产保存信息并发送至存储服务系统,其中,所述托管资产保存信息包括资产托管上链请求信息和所述资产权利托管转让信息,所述资产托管上链请求信息包括链下资产托管转让请求信息和托管资产发行信息;

所述存储服务系统接收并存储所述托管资产保存信息,之后将带有所述存储服务系统签名的托管资产登记索引信息反馈至所述资产托管系统;其中,所述托管资产登记索引信息包括托管资产登记索引标识和所述托管资产保存信息的防篡改信息;

所述资产托管系统向资产账本系统发送带有所述资产托管系统签名的托管资产发行请求信息,其中,所述托管资产发行请求信息包括带有所述存储服务系统签名的托管资产

登记索引信息和所述托管资产发行信息；

所述资产账本系统对所述托管资产发行请求信息进行验证，验证通过后，将所述托管资产发行请求信息记录到包含资产权利人的资产账本地址的初始块信息中。

10. 根据权利要求9所述的方法，其特征在于，当所述防篡改信息为对所述托管资产保存信息进行哈希运算得到的哈希值的情况下，所述方法还包括：

所述资产托管系统根据所述托管资产登记索引信息的托管资产登记索引标识，从所述存储服务系统中获取对应的托管资产保存信息；

对获取的所述托管资产保存信息进行哈希运算得到第二哈希值，将所述第二哈希值与所述托管资产登记索引信息包含的防篡改信息进行比较；以及

根据比较结果判断所述托管资产保存信息是否被篡改。

11. 根据权利要求9所述的方法，其特征在于，当所述防篡改信息为对所述托管资产保存信息进行哈希运算得到哈希值后，使用所述资产托管系统和所述存储服务系统的私钥分别对所述哈希值进行签名得到的结果的情况下，所述方法还包括：

所述资产托管系统根据所述托管资产登记索引信息的托管资产登记索引标识，从所述存储服务系统中获取对应的托管资产保存信息；

对获取的所述托管资产保存信息进行哈希运算得到第二哈希值，使用所述资产托管系统和所述存储服务系统的公钥分别与对应的私钥签名进行验证；以及

根据验证结果判断所述托管资产保存信息是否被篡改。

12. 根据权利要求9至11的任一项所述的方法，其特征在于，所述方法还包括：

资产应用终端系统基于所述资产权利人选择和/或输入的查询要求以及所述资产权利人对应的资产账本地址，生成第一链上资产查询请求信息，之后将所述第一链上资产查询请求信息发送至所述资产账本系统；

所述资产账本系统根据所述第一链上资产查询请求信息的资产账本地址，查询与所述资产账本地址相对应的链上资产信息以及与所述链上资产信息的托管资产类别相对应的初始块信息，之后反馈至所述资产应用终端系统；

所述资产应用终端系统基于所述资产权利人选择的所述初始块信息对应的托管资产登记索引标识，生成第二链上资产查询请求信息，之后将所述第二链上资产查询请求信息发送至存储服务系统；

所述存储服务系统根据所述第二链上资产查询请求信息的托管资产登记索引标识，查询与所述托管资产登记索引标识相对应的托管资产保存信息，之后反馈至所述资产应用终端系统。

一种基于区块链的数字资产存储系统和方法

技术领域

[0001] 本发明涉及数字资产技术领域,尤其涉及一种基于区块链的数字资产存储系统和方法。

背景技术

[0002] 目前区块链技术发展迅速,区块链作为一个去中心化的新型分布式计算范式,为各种数字资产在分布式网络上的运行提供了技术支持。这些数字资产运行在区块链的分布式网络上,不依赖某个特定第三方或中心方记账,而通过共享账本方式进行全局多节点共识记账,并通过加密算法实现了一种技术保障的安全体系。

[0003] 在实现本发明过程中,发明人发现现有技术中至少存在如下问题:

[0004] 如果在区块链上存储大量信息会导致链上存储空间膨胀,整个区块链的运行性能下降,因而现有技术中无法提供资产信息登记服务。

发明内容

[0005] 有鉴于此,本发明实施例提供一种基于区块链的数字资产存储系统和方法,通过将托管资产的信息中的托管资产保存信息保存到链下的存储服务系统,将托管资产登记索引信息保存到链上的资产账本系统,在保证区块链运行性能的前提下,实现了链上信息的轻量化存储。

[0006] 为实现上述目的,根据本发明实施例的一个方面,提供了一种基于区块链的数字资产存储系统。

[0007] 根据本发明实施例的基于区块链的数字资产存储系统,包括:资产托管系统、资产账本系统和存储服务系统;其中,所述资产托管系统,用于接收带有资产应用终端系统签名的资产权利托管转让信息,以生成托管资产保存信息并发送至所述存储服务系统,其中,所述托管资产保存信息包括资产托管上链请求信息和所述资产权利托管转让信息,所述资产托管上链请求信息包括链下资产托管转让请求信息和托管资产发行信息;所述存储服务系统,用于接收并存储所述托管资产保存信息,之后将带有所述存储服务系统签名的托管资产登记索引信息反馈至所述资产托管系统;其中,所述托管资产登记索引信息包括托管资产登记索引标识和所述托管资产保存信息的防篡改信息;所述资产托管系统,还用于向所述资产账本系统发送带有所述资产托管系统签名的托管资产发行请求信息,其中,所述托管资产发行请求信息包括带有所述存储服务系统签名的托管资产登记索引信息和所述托管资产发行信息;所述资产账本系统,用于对所述托管资产发行请求信息进行验证,验证通过后,将所述托管资产发行请求信息记录到包含资产权利人的资产账本地址的初始块信息中。

[0008] 可选地,所述防篡改信息为:所述托管资产保存信息的数字指纹信息,或利用所述资产托管系统和所述存储服务系统对所述数字指纹信息进行签名后的信息。

[0009] 可选地,所述资产托管系统还用于:根据所述链下资产托管转让请求信息和所述

托管资产发行信息,生成所述资产托管上链请求信息,之后将带有所述资产托管系统签名的资产托管上链请求信息发送至所述资产应用终端系统;所述资产应用终端系统,用于使用身份证书对应的用户私钥对所述资产托管上链请求信息进行签名,之后反馈至所述资产托管系统。

[0010] 可选地,所述资产托管系统还用于:接收来自所述资产应用终端系统的带有所述资产应用终端系统签名的资产权利托管转让信息,添加所述资产托管系统的签名后发送至资产托管方;接收来自所述资产托管方的带有所述资产托管方签名的资产权利托管转让信息;其中,所述资产权利托管转让信息包括资产权利转让凭证信息、所述资产托管方持有资产的凭证信息、更新的链下资产登记信息。

[0011] 可选地,所述对所述托管资产发行请求信息进行验证,包括:验证所述托管资产发行请求信息的签名,以及所述托管资产登记索引信息的签名;验证通过后,根据所述托管资产登记索引信息的托管资产登记索引标识从所述存储服务系统中获取对应的托管资产保存信息;验证所述托管资产保存信息的防篡改信息,所述托管资产权利转让信息的三方签名,以及所述托管资产上链请求信息的双签名;其中,所述三方签名为所述资产托管系统、所述资产托管方和所述资产应用终端系统的签名,所述双签名为所述资产托管系统和所述资产应用终端系统的签名;验证所述托管资产发行信息的权利人地址,与所述链下资产托管转让请求信息的实名账本记录中的资产账本地址是否一致。

[0012] 可选地,当所述防篡改信息为对所述托管资产保存信息进行哈希运算得到的哈希值的情况下,所述资产托管系统,还用于:根据所述托管资产登记索引信息的托管资产登记索引标识,从所述存储服务系统中获取对应的托管资产保存信息;对获取的所述托管资产保存信息进行哈希运算得到第二哈希值,将所述第二哈希值与所述托管资产登记索引信息包含的防篡改信息进行比较;根据比较结果判断所述托管资产保存信息是否被篡改。

[0013] 可选地,当所述防篡改信息为对所述托管资产保存信息进行哈希运算得到哈希值后,使用所述资产托管系统和所述存储服务系统的私钥分别对所述哈希值进行签名得到的结果的情况下,所述资产托管系统,还用于:根据所述托管资产登记索引信息的托管资产登记索引标识,从所述存储服务系统中获取对应的托管资产保存信息;对获取的所述托管资产保存信息进行哈希运算得到第二哈希值,使用所述资产托管系统和所述存储服务系统的公钥分别与对应的私钥签名进行验证;根据验证结果判断所述托管资产保存信息是否被篡改。

[0014] 可选地,所述系统还包括:资产应用终端系统;其中,所述资产应用终端系统,用于基于所述资产权利人选择和/或输入的查询要求以及所述资产权利人对应的资产账本地址,生成第一链上资产查询请求信息,之后将所述第一链上资产查询请求信息发送至所述资产账本系统;所述资产账本系统,还用于根据所述第一链上资产查询请求信息的资产账本地址,查询与所述资产账本地址相对应的链上资产信息以及与所述链上资产信息的托管资产类别相对应的初始块信息,之后反馈至所述资产应用终端系统;所述资产应用终端系统,还用于基于所述资产权利人选择的所述初始块信息对应的托管资产登记索引标识,生成第二链上资产查询请求信息,之后将所述第二链上资产查询请求信息发送至存储服务系统;所述存储服务系统,还用于根据所述第二链上资产查询请求信息的托管资产登记索引标识,查询与所述托管资产登记索引标识相对应的托管资产保存信息,之后反馈至所述资

产应用终端系统。

[0015] 根据本发明实施例的另一个方面,提供一种基于区块链的数字资产存储方法。

[0016] 根据本发明实施例的基于区块链的数字资产存储方法,包括:资产托管系统接收带有资产应用终端系统签名的资产权利托管转让信息,以生成托管资产保存信息并发送至存储服务系统,其中,所述托管资产保存信息包括资产托管上链请求信息和所述资产权利托管转让信息,所述资产托管上链请求信息包括链下资产托管转让请求信息和托管资产发行信息;所述存储服务系统接收并存储所述托管资产保存信息,之后将带有所述存储服务系统签名的托管资产登记索引信息反馈至所述资产托管系统;其中,所述托管资产登记索引信息包括托管资产登记索引标识和所述托管资产保存信息的防篡改信息;所述资产托管系统向资产账本系统发送带有所述资产托管系统签名的托管资产发行请求信息,其中,所述托管资产发行请求信息包括带有所述存储服务系统签名的托管资产登记索引信息和所述托管资产发行信息;所述资产账本系统对所述托管资产发行请求信息进行验证,验证通过后,将所述托管资产发行请求信息记录到包含资产权利人的资产账本地址的初始块信息中。

[0017] 可选地,当所述防篡改信息为对所述托管资产保存信息进行哈希运算得到的哈希值的情况下,所述方法还包括:所述资产托管系统根据所述托管资产登记索引信息的托管资产登记索引标识,从所述存储服务系统中获取对应的托管资产保存信息;对获取的所述托管资产保存信息进行哈希运算得到第二哈希值,将所述第二哈希值与所述托管资产登记索引信息包含的防篡改信息进行比较;以及根据比较结果判断所述托管资产保存信息是否被篡改。

[0018] 可选地,当所述防篡改信息为对所述托管资产保存信息进行哈希运算得到哈希值后,使用所述资产托管系统和所述存储服务系统的私钥分别对所述哈希值进行签名得到的结果的情况下,所述方法还包括:所述资产托管系统根据所述托管资产登记索引信息的托管资产登记索引标识,从所述存储服务系统中获取对应的托管资产保存信息;对获取的所述托管资产保存信息进行哈希运算得到第二哈希值,使用所述资产托管系统和所述存储服务系统的公钥分别与对应的私钥签名进行验证;以及根据验证结果判断所述托管资产保存信息是否被篡改。

[0019] 可选地,所述方法还包括:资产应用终端系统基于所述资产权利人选择和/或输入的查询要求以及所述资产权利人对应的资产账本地址,生成第一链上资产查询请求信息,之后将所述第一链上资产查询请求信息发送至所述资产账本系统;所述资产账本系统根据所述第一链上资产查询请求信息的资产账本地址,查询与所述资产账本地址相对应的链上资产信息以及与所述链上资产信息的托管资产类别相对应的初始块信息,之后反馈至所述资产应用终端系统;所述资产应用终端系统基于所述资产权利人选择的所述初始块信息对应的托管资产登记索引标识,生成第二链上资产查询请求信息,之后将所述第二链上资产查询请求信息发送至存储服务系统;所述存储服务系统根据所述第二链上资产查询请求信息的托管资产登记索引标识,查询与所述托管资产登记索引标识相对应的托管资产保存信息,之后反馈至所述资产应用终端系统。

[0020] 上述发明中的一个实施例具有如下优点或有益效果:通过将托管资产的信息中的托管资产保存信息保存到链下的存储服务系统,将托管资产登记索引信息保存到链上的资

产账本系统,在保证区块链运行性能的前提下,实现了链上信息的轻量化存储;通过将托管资产登记索引信息中的防篡改信息与存储服务系统中的托管资产保存信息生成的防篡改信息进行比较,以保证托管资产保存信息是真实未被篡改的;基于该轻量化存储方式,如果需要查询托管资产保存信息,需先在资产账本系统中查询到初始块中的托管资产登记索引信息,再基于托管资产登记索引信息中的托管资产登记索引标识查询到托管资产保存信息;查询到托管资产保存信息后,可采用防篡改信息进行验证,保证信息真实未被篡改。

[0021] 上述的非惯用的可选方式所具有的进一步效果将在下文中结合具体实施方式加以说明。

附图说明

[0022] 附图用于更好地理解本发明,不构成对本发明的不当限定。其中:

[0023] 图1是本发明实施例一中基于区块链的数字资产存储系统的主要子系统示意图;

[0024] 图2是本发明实施例一中基于区块链的数字资产存储系统进行信息存储的主要流程示意图;

[0025] 图3是本发明实施例四中基于区块链的数字资产存储系统进行信息查询的主要流程示意图;

[0026] 图4是本发明实施例中基于区块链的数字资产存储方法的主要流程示意图。

具体实施方式

[0027] 以下结合附图对本发明的示范性实施例做出说明,其中包括本发明实施例的各种细节以助于理解,应当将它们认为仅仅是示范性的。因此,本领域普通技术人员应当认识到,可以对这里描述的实施例做出各种改变和修改,而不会背离本发明的范围和精神。同样,为了清楚和简明,以下的描述中省略了对公知功能和结构的描述。

[0028] 图1是本发明实施例一中基于区块链的数字资产存储系统的主要子系统示意图。如图1所示,本发明实施例一的基于区块链的数字资产存储系统100,主要包括:

[0029] 资产托管系统101,用于接收带有资产应用终端系统签名的资产权利托管转让信息,以生成托管资产保存信息并发送至存储服务系统,其中,所述托管资产保存信息包括资产托管上链请求信息和资产权利托管转让信息,所述资产托管上链请求信息包括链下资产托管转让请求信息和包括托管资产描述信息的托管资产发行信息。托管资产保存信息可以认为是在存储服务系统中存放的、与链下资产托管上链或链上资产下链返还相关的、证实资产托管方作为托管资产权利人的全面的托管资产信息;托管资产描述信息是对托管资产保存信息的概要描述。其中,链下资产托管转让请求信息包括:链下资产托管转让请求指令和实名账本记录。链下资产托管转让请求指令包括:链下资产登记信息、托管转让资产金额或数量。链下资产登记信息是指用户在资产权利登记系统中登记的链下资产信息,例如用户拥有哪些类型的资产、每种类型资产的金额或数量、资产的相关状态信息(例如是否质押、是否存在瑕疵等)等;托管转让资产金额或数量是指,用户请求托管转让的链下资产的金额或数量。在可选的实施例中,链下资产登记信息包括:资产权利登记系统的访问地址、资产识别信息(包括资产权利人的身份标识、资产类别、资产标识或编号、资产金额或数量)。实名账本记录包括:与用户的身份信息相关联的身份证书(包括用户的身份标识和用

户公钥)和与用户的身份信息相关联的资产账本地址。

[0030] 托管资产发行信息是指将链下资产托管至链上时的发行信息,资产托管方信息是指负责托管发行至链上的链下资产的资产托管方的信息。在可选的实施例,托管资产发行信息包括:托管资产类别、托管资产描述信息、权利人地址、资产发行单位数量等。资产权利托管转让信息包括:资产权利转让凭证信息、资产托管方持有资产的凭证信息、更新的链下资产登记信息、其它资产描述和登记信息等。此处的凭证信息可以是纸质文件电子化的凭证信息,也可以是纯电子化的凭证信息,比如电子签名存档。

[0031] 存储服务系统102,用于接收并存储所述托管资产保存信息,之后将带有所述存储服务系统签名的托管资产登记索引信息反馈至所述资产托管系统;其中,所述托管资产登记索引信息包括托管资产登记索引标识和所述托管资产保存信息的防篡改信息。该防篡改信息比如可以是对托管资产保存信息进行哈希运算得到的哈希值,防篡改信息用于校验托管资产保存信息,防止其被篡改。

[0032] 资产托管系统101,还用于向资产账本系统发送带有所述资产托管系统签名的托管资产发行请求信息,其中,所述托管资产发行请求信息包括带有所述存储服务系统签名的托管资产登记索引信息和所述托管资产发行信息。资产托管系统基于托管资产登记索引信息和托管资产发行信息生成托管资产发行请求信息,之后将带有资产托管系统签名的托管资产发行请求信息发送至资产账本系统。

[0033] 资产账本系统103,用于对所述托管资产发行请求信息进行验证,验证通过后,将所述托管资产发行请求信息记录到包含资产权利人的资产账本地址的初始块信息中。验证内容包括:托管资产发行请求信息的签名、托管资产登记索引信息的签名、托管资产保存信息的防篡改信息、托管资产权利转让信息的签名、托管资产上链请求信息的签名;以及验证托管资产发行信息的权利人地址,与链下资产托管转让请求信息的实名账本记录中的资产账本地址是否一致。验证通过后,即可将托管资产发行请求信息记录到资产权利人的资产账本地址对应的初始块信息中。

[0034] 图2是本发明实施例一中基于区块链的数字资产存储系统进行信息存储的主要流程示意图。如图2所示,本发明实施例一的基于区块链的数字资产存储系统进行信息存储的主要流程,包括以下步骤:

[0035] 步骤S201:资产托管系统根据链下资产托管转让请求信息和托管资产发行信息,生成资产托管上链请求信息,之后将带有资产托管系统签名的资产托管上链请求信息发送至资产应用终端系统。资产托管系统可以是对用户将链下的实名登记资产通过指定的资产托管方进行托管登记管理、以及对托管资产在区块链上发行数字资产的过程进行登记管理的系统,用户可以通过Web或其它方式对该资产托管系统进行访问,发行数字资产的过程包括链下资产上链流程和链上资产下链流程。其中,链下资产上链,即是用户将用户在区块链之下的实名资产通过资产托管方托管后,由资产托管系统向基于区块链的资产账本系统发行链上数字资产;链上资产下链,即是用户将用户在区块链上的数字资产作废,并将该数字资产对应的链下托管资产返还转让至用户。其中,所述资产托管上链请求信息包括链下资产托管转让请求信息和包括托管资产描述信息的托管资产发行信息。上述各信息中包含的具体内容见对于资产托管系统101的详细说明。托管资产发行信息中的托管资产类别与链下资产托管转让请求信息中对应的资产识别信息中的资产类别相同。

[0036] 需要注意的是,本发明实施例中预先将数字资产进行分类处理,每类数字资产对应唯一的资产类别。数字资产包括可分割的数字资产和不可分割的数字资产,可分割的数字资产是指对初始块包含的托管资产在链下可以分割,比如股票、黄金等;不可分割的数字资产是指对初始块包含的托管资产在链下不可以分割,比如房屋、文物、著作权、金融合同等。当两份资产属于同一种类可分割的数字资产时,这两份资产之间可以进行运算。两份不可分割的数字资产即使属于同一种类,这两份资产之间也是不可以进行运算的,比如,数字资产房产A与数字资产房产B,虽然都属于房产类,但这两份资产之间不可以进行运算。使用资产类别可以明确该类资产是属于可分割的数字资产还是不可分割的数字资产,便于下链清算。

[0037] 步骤S202:资产应用终端系统使用身份证书的用户公钥对应的用户私钥,对带有资产托管系统签名的资产托管上链请求信息进行签名,之后反馈至资产托管系统。资产应用终端系统是安装在终端设备上的与资产账本系统对应的系统软件;用户可以通过访问资产托管系统,从资产托管系统上下载并安装资产应用终端系统软件。终端设备可以是具有显示屏并且支持网页浏览的各种电子设备,比如手机、平板电脑、台式计算机等。身份证书可以是信息不可抵赖提供的CA(Certification Authority,证书授权中心)证书。经步骤S201和步骤S202处理,得到了带有资产托管系统和资产应用终端系统双签名的资产托管上链请求信息。

[0038] 用户的密钥对可以由资产应用终端系统在本地采用不对称加密算法生成。用户的密钥对包括用户私钥和用户公钥,可以根据用户公钥确定用户的区块链钱包中的资产账本地址。用户私钥可以用于对用户身份信息、用户的银行卡信息、用户的生物识别码信息或用户的身份证书等数据信息进行签名,也可以在后续资产交易或融资流程中用于对数字资产信息进行签名,以确认交易的所有权。用户公钥可以用于对被该用户私钥进行签名过的数据信息进行相应的验证。

[0039] 在一优选的实施例中,资产应用终端系统在接收到带有资产托管系统签名的资产托管上链请求信息后,可以先通过终端设备展示给用户,以使用户在终端设备上确认资产托管上链请求信息,之后再执行步骤S202。

[0040] 步骤S203:资产托管系统使用身份证书对资产托管上链请求信息的签名进行验证,验证通过后,登记带有用户私钥签名的资产托管上链请求信息,并将其发送至资产应用终端系统和资产托管方。所述资产托管上链请求信息是指用户对于自己拥有的链下资产,可以发起资产托管上链的请求。验证签名,用于确认该资产托管上链请求信息有效、可信。若验证未通过,则资产应用终端系统返回错误信息。若验证通过,将带有用户私钥签名的资产托管上链请求信息发送至资产托管方。

[0041] 步骤S204:资产权利人通过资产应用终端系统向资产权利登记系统发起办理权利转让给资产托管方的操作,权利转让完成后,向资产应用终端系统确认完成资产托管转让操作信息。

[0042] 步骤S205:资产应用终端系统向资产托管系统发送带有资产应用终端系统签名的资产权利托管转让信息。根据资产托管上链请求信息的链下资产托管转让请求信息的链下资产托管转让请求指令的链下资产登记信息和托管转让资产金额或数量,向资产权利登记系统发起办理权利转让给资产托管方的操作。资产托管方可以是具备一定资格的、具有一

定公信力度的机构,比如商业银行以及其业务系统;资产托管方可以是一个用于接收托管资产的实体,可以采用基金等法律关系成立;在一些实际情况中,该实体可以采用人工方式来处理信息。资产权利登记系统为链下传统的资产权利登记系统。

[0043] 步骤S206:资产托管系统验证资产权利托管转让信息的签名后,将带有资产托管系统签名的资产权利托管转让信息发送至资产托管方。

[0044] 步骤S207:资产托管方对资产权利托管转让信息进行验证,验证通过后,将带有资产托管方的资产权利托管转让信息进行签名,之后发送至资产托管系统。经步骤S204至步骤S207处理,得到了带有资产托管系统、资产托管方和资产应用终端系统三方签名的资产权利托管转让信息,这样相当于参与方都确认过资产权利托管转让信息,防止出现差错。本实施例中所涉及的资产权利人相当于用户。

[0045] 步骤S208:资产托管系统基于签名的资产托管上链请求信息和资产权利托管转让信息,生成托管资产保存信息并发送至存储服务系统。此处的托管资产保存信息可以认为是在存储服务系统中存放的、与链下资产托管上链或链上资产下链返还相关的、证实资产托管方作为托管资产权利人的全面的托管资产信息,在可选的实施例中,所述托管资产保存信息包括带有双签名的资产托管上链请求信息、以及带有三方签名的资产权利托管转让信息。实施例中的存储服务系统需要安全可信,可以是云存储服务系统,也可以是一台具有存储功能的设备,也可以是由多台具有存储功能的设备通过网络连接形成的系统。

[0046] 步骤S209:存储服务系统接收并存储托管资产保存信息,之后将带有存储服务系统签名的托管资产登记索引信息反馈至资产托管系统。其中,托管资产登记索引信息包括托管资产登记索引标识和托管资产保存信息的防篡改信息。所述防篡改信息为:托管资产保存信息的数字指纹信息,或利用资产托管系统和存储服务系统对所述数字指纹信息进行签名后的信息。数字指纹信息是指采用某种算法对托管资产保存信息进行运算得到的信息,例如,对托管资产保存信息进行哈希运算后得到的哈希值。需要说明的是,数字指纹信息也可以采用其他算法对托管资产保存信息进行运算得到的信息,只要运算得到的信息唯一对应一个托管资产保存信息即可。

[0047] 步骤S210:资产托管系统接收到带有存储服务系统签名的托管资产登记索引信息后,将带有资产托管系统签名的托管资产发行请求信息发送至资产账本系统。其中,托管资产发行请求信息包括带有存储服务系统签名的托管资产登记索引信息和托管资产发行信息。

[0048] 步骤S211:资产账本系统对托管资产发行请求信息进行验证,验证通过后,将托管资产发行请求信息记录到资产权利人的资产账本地址对应的初始块信息中。资产账本系统是基于区块链技术的资产账本系统,可以由其上的链上共识节点进行验证、查询、记录等操作。资产账本系统对托管资产发行请求信息进行验证的具体实现为:验证托管资产发行请求信息的签名、托管资产登记索引信息的签名;根据托管资产登记索引信息的托管资产登记索引标识从存储服务系统中获取对应的托管资产保存信息,验证托管资产保存信息的防篡改信息、托管资产权利转让信息的三方签名、托管资产上链请求信息的双签名;以及验证托管资产发行信息的权利人地址,与链下资产托管转让请求信息的实名账本记录中的资产账本地址是否一致。验证防篡改信息,用于确保托管资产保存信息未被篡改。

[0049] 验证通过后,即可将托管资产发行请求信息记录到资产权利人的资产账本地址对

应的初始块信息中。此处的初始块信息包括：初始块块号、带有资产托管系统签名的托管资产发行请求信息等。

[0050] 实施例二：由实施例一的步骤S201、步骤S202可知，在生成资产托管上链请求信息后，先由资产托管系统对资产托管上链请求信息签名后，再发送至资产应用终端系统签名，最终形成双签名的资产托管上链请求信息。同样地，可以先由资产应用终端系统对资产托管上链请求信息签名后，再发送至资产托管系统签名，最终也会形成双签名的资产托管上链请求信息。实施例一的上述两个步骤可以由下述过程代替：

[0051] (1) 资产托管系统根据链下资产托管转让请求信息和托管资产发行信息，生成资产托管上链请求信息，之后发送至资产应用终端系统。

[0052] (2) 资产应用终端系统使用身份证书的用户公钥对应的用户私钥，对资产托管上链请求信息进行签名，之后反馈至资产托管系统。

[0053] (3) 资产托管系统对带有资产应用终端系统签名的资产托管上链请求信息进行签名。

[0054] 实施例三：实施例一、实施例二中的数字资产存储系统均实现了信息的轻量化存储，后续还可以通过防篡改信息对该数字资产存储系统存储的托管资产保存信息进行验证，防止其被篡改。防篡改信息的获得有多种实现方式，每种实现方式的验证过程有差别，下面按照实现方式的不同分别进行说明。

[0055] 对于防篡改信息为对托管资产保存信息进行哈希运算得到的哈希值这一情况，验证过程的具体实现如下：

[0056] (1) 资产托管系统根据托管资产登记索引信息的托管资产登记索引标识，从存储服务系统中获取对应的托管资产保存信息；

[0057] (2) 资产托管系统对获取的托管资产保存信息进行哈希运算得到第二哈希值，将第二哈希值与第一哈希值进行比较，根据比较结果判断托管资产保存信息是否被篡改。其中，第一哈希值即为托管资产登记索引信息包含的防篡改信息。如果第二哈希值与第一哈希值相同，说明存储服务系统保存的托管资产保存信息是真实未被篡改的；否则，说明已被篡改。

[0058] 对于防篡改信息为对托管资产保存信息进行哈希运算得到哈希值后，使用资产托管系统和存储服务系统的私钥分别对该哈希值进行签名的结果这一情况，验证过程的具体实现如下：

[0059] (1) 资产托管系统根据托管资产登记索引信息的托管资产登记索引标识，从存储服务系统中获取对应的托管资产保存信息；

[0060] (2) 资产托管系统对获取的托管资产保存信息进行哈希运算得到第二哈希值，使用资产托管系统和存储服务系统的公钥分别与各自对应的私钥签名进行验证，以判断托管资产保存信息是否被篡改。

[0061] 对于托管资产保存信息更新的情况，对应资产下链过程，资产账本系统中保存的托管资产登记索引信息中应包括更新后托管资产描述信息和更新后的托管资产保存信息的防篡改信息。实施例中，资产账本系统和存储服务系统均采用追加方式更新信息，更新内容包括更新前和更新后对应信息的托管资产登记索引标识和防篡改信息。实施例中，可以从最新的信息开始，通过资产账本系统的区块链式结构向前检索至初始块记录和终结块记

录(若下链),该初始块记录包含托管资产登记索引信息,该终结块记录包含更新的托管资产登记索引信息。基于上述托管资产登记索引信息包含的托管资产登记索引标识,从存储服务系统查询托管资产保存信息,并通过该托管资产登记索引信息的防篡改信息验证所查询的托管资产保存信息是否是真实未被篡改的。

[0062] 实施例四:实施例一中的数字资产存储系统实现了信息的轻量化存储,后续查询该数字资产存储系统中的托管资产保存信息时,需先在资产账本系统中查询到初始块中的托管资产描述信息,再基于托管资产描述信息中的托管资产登记索引标识查询到托管资产保存信息。具体实现如下:

[0063] 图3是本发明实施例四中基于区块链的数字资产存储系统进行信息查询的主要流程示意图。如图3所示,本发明实施例四的基于区块链的数字资产存储系统进行信息查询的主要流程,包括以下步骤:

[0064] 步骤S301:资产应用终端系统基于资产权利人选择和/或输入的查询要求以及资产权利人对应的资产账本地址,生成第一链上资产查询请求信息,之后将第一链上资产查询请求信息发送至资产账本系统。资产权利人在资产应用终端系统的链上资产查询功能界面中输入和/或选择查询要求,资产应用终端系统基于查询要求生成第一链上资产查询请求信息后,发送至资产账本系统。其中,第一链上资产查询请求信息是指用户对于自己已上链的数字资产,可以发起数字资产查询的请求;查询要求是指用户进行链上资产查询可能用到的一些限制因素,可以包括:查询条件和查询结果,所述查询条件可以包括:资产序号、资产类别、资产状态,所述查询结果可以包括:所述资产数量、资产明细、初始块信息、终结块信息、资产交易历史记录、初始块对应的托管资产保存信息、终结块对应的托管资产保存信息。本实施例中为了获取托管资产保存信息,查询要求至少包括初始块对应的托管资产保存信息,其他项可根据需求自行设置。

[0065] 步骤S302:资产账本系统根据所述第一链上资产查询请求信息的资产账本地址,查询与所述资产账本地址相对应的链上资产信息以及与所述链上资产信息的托管资产类别相对应的初始块信息,之后反馈至所述资产应用终端系统。其中,链上资产信息包括:资产账本地址、托管资产类别、资产数量、资产记录索引和关联资产信息等。

[0066] 步骤S303:资产应用终端系统将查询出的与链上资产信息的托管资产类别相对应的初始块信息通过终端设备展示给用户。

[0067] 步骤S304:资产应用终端系统基于资产权利人选择的初始块信息对应的托管资产登记索引标识,生成第二链上资产查询请求信息,之后将第二链上资产查询请求信息发送至存储服务系统。用户根据查询出的初始块信息,在链上资产查询功能界面中选择该初始块信息对应的托管资产登记索引标识,资产应用终端系统基于托管资产登记索引标识生成第二链上资产查询请求信息后,发送至存储服务系统。

[0068] 步骤S305:存储服务系统根据第二链上资产查询请求信息的托管资产登记索引标识,查询与托管资产登记索引标识相对应的托管资产保存信息,之后反馈至资产应用终端系统。资产应用终端系统访问存储服务系统,查询与初始块信息的托管资产发行请求中的托管资产登记索引信息中的托管资产登记索引标识相对应的托管资产保存信息,存储服务系统将查询结果反馈至资产应用终端系统。

[0069] 步骤S306:资产应用终端系统验证托管资产保存信息中的签名,验证通过后,将资

产类别对应的托管资产保存信息通过终端设备展示给用户。实施例中,资产应用终端系统可以将每一个资产类别对应的托管资产保存信息展示给用户。

[0070] 在一优选的实施例中,当查询到托管资产保存信息后,即可按照实施例三的方式对该托管资产保存信息进行验证,防止其被篡改。

[0071] 图4是本发明实施例中基于区块链的数字资产存储方法的主要流程示意图。如图4所示本发明实施例中基于区块链的数字资产存储方法,主要包括以下步骤:

[0072] 步骤S401:资产托管系统接收带有资产应用终端系统签名的资产权利托管转让信息,以生成托管资产保存信息并发送至存储服务系统,其中,所述托管资产保存信息包括资产托管上链请求信息和资产权利托管转让信息,所述资产托管上链请求信息包括链下资产托管转让请求信息和包括托管资产描述信息的托管资产发行信息。托管资产保存信息可以认为是在存储服务系统中存放的、与链下资产托管上链或链上资产下链返还相关的、证实资产托管方作为托管资产权利人的全面的托管资产信息;托管资产描述信息是对托管资产保存信息的概要描述。其中,链下资产托管转让请求信息包括:链下资产托管转让请求指令和实名账本记录。链下资产托管转让请求指令包括:链下资产登记信息、托管转让资产金额或数量。链下资产登记信息是指用户在资产权利登记系统中登记的链下资产信息,例如用户拥有哪些类型的资产、每种类型资产的金额或数量、资产的相关状态信息(例如是否质押、是否存在瑕疵等)等;托管转让资产金额或数量是指,用户请求托管转让的链下资产的金额或数量。在可选的实施例中,链下资产登记信息包括:资产权利登记系统的访问地址、资产识别信息(包括资产权利人身份标识、资产类别、资产标识或编号、资产金额或数量)。实名账本记录包括与用户的身份信息相关联的身份证书(包括用户的身份标识和用户公钥)和与用户的身份信息相关联的资产账本地址。

[0073] 托管资产发行信息是指将链下资产托管至链上时的发行信息,资产托管方信息是指负责托管发行至链上的链下资产的资产托管方的信息。在可选的实施例中,托管资产发行信息包括:托管资产类别、托管资产描述信息、权利人地址、资产发行单位数量等。资产权利托管转让信息包括:资产权利转让凭证信息、资产托管方持有资产的凭证信息、更新的链下资产登记信息、其它资产描述和登记信息等。此处的凭证信息可以是纸质文件电子化的凭证信息,也可以是纯电子化的凭证信息,比如电子签名存档。

[0074] 步骤S402:所述存储服务系统接收并存储所述托管资产保存信息,之后将带有所述存储服务系统签名的托管资产登记索引信息反馈至所述资产托管系统;其中,所述托管资产登记索引信息包括托管资产登记索引标识和所述托管资产保存信息的防篡改信息。该防篡改信息比如可以是对托管资产保存信息进行哈希运算得到的哈希值,防篡改信息用于校验托管资产保存信息,防止其被篡改。

[0075] 步骤S403:所述资产托管系统向资产账本系统发送带有所述资产托管系统签名的托管资产发行请求信息,其中,所述托管资产发行请求信息包括带有所述存储服务系统签名的托管资产登记索引信息和所述托管资产发行信息。资产托管系统基于托管资产登记索引信息和托管资产发行信息生成托管资产发行请求信息,之后将带有资产托管系统签名的托管资产发行请求信息发送至资产账本系统。

[0076] 步骤S404:所述资产账本系统对所述托管资产发行请求信息进行验证,验证通过后,将所述托管资产发行请求信息记录到资产权利人的资产账本地址对应的初始块信息

中。验证内容包括：托管资产发行请求信息的签名、托管资产登记索引信息的签名、托管资产保存信息的防篡改信息、托管资产权利转让信息的签名、托管资产上链请求信息的签名；以及验证托管资产发行信息的权利人地址，与链下资产托管转让请求信息的实名账本记录中的资产账本地址是否一致。验证通过后，即可将托管资产发行请求信息记录到资产权利人的资产账本地址对应的初始块信息中。

[0077] 根据本发明实施例的技术方案，通过将托管资产的信息中的托管资产保存信息保存到链下的存储服务系统，将托管资产登记索引信息保存到链上的资产账本系统，在保证区块链运行性能的前提下，实现了链上信息的轻量化存储；通过将托管资产登记索引信息中的防篡改信息与存储服务系统中的托管资产保存信息生成的防篡改信息进行比较，以保证托管资产保存信息是真实未被篡改的；基于该轻量化存储方式，如果需要查询托管资产保存信息，需先在资产账本系统中查询到初始块中的托管资产登记索引信息，再基于托管资产登记索引信息中的托管资产登记索引标识查询到托管资产保存信息；查询到托管资产保存信息后，可采用防篡改信息进行验证，保证信息真实未被篡改。

[0078] 上述具体实施方式，并不构成对本发明保护范围的限制。本领域技术人员应该明白的是，取决于设计要求和因素，可以发生各种各样的修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明保护范围之内。

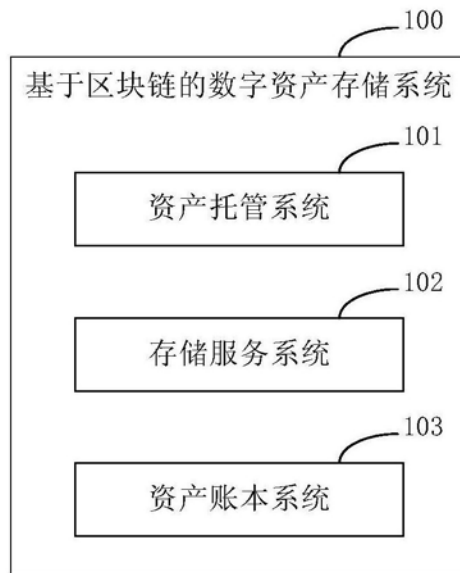


图1

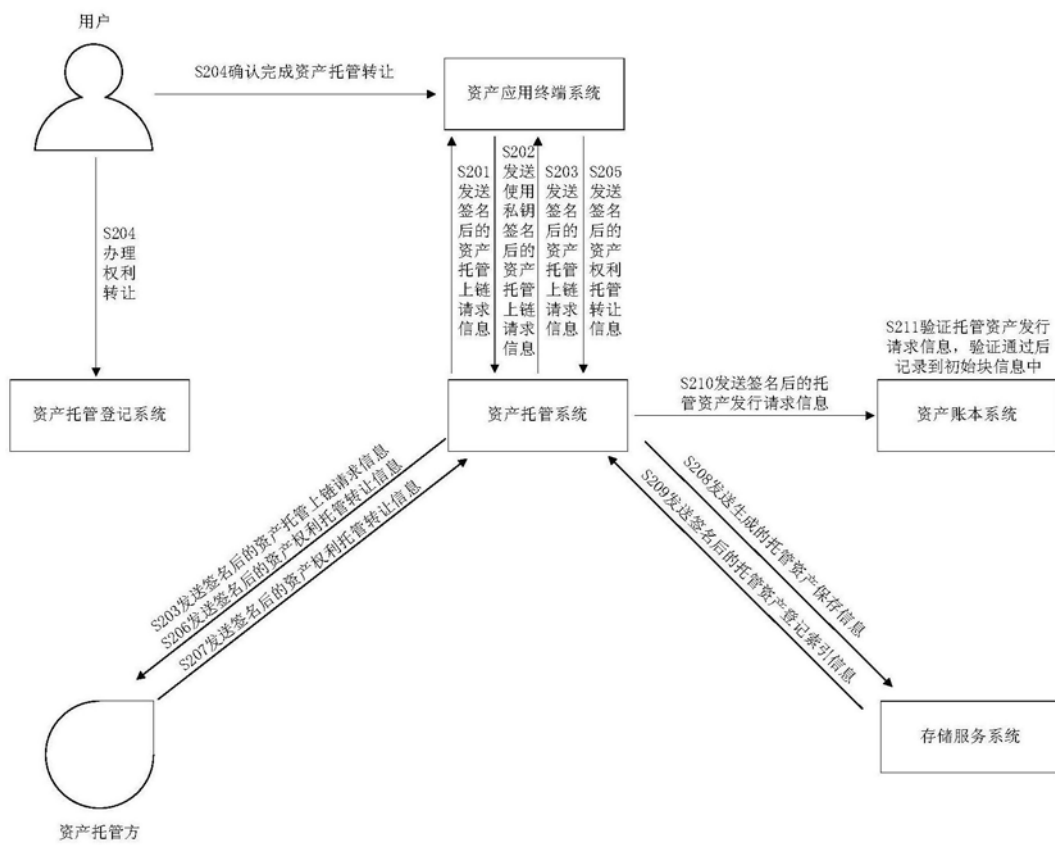


图2

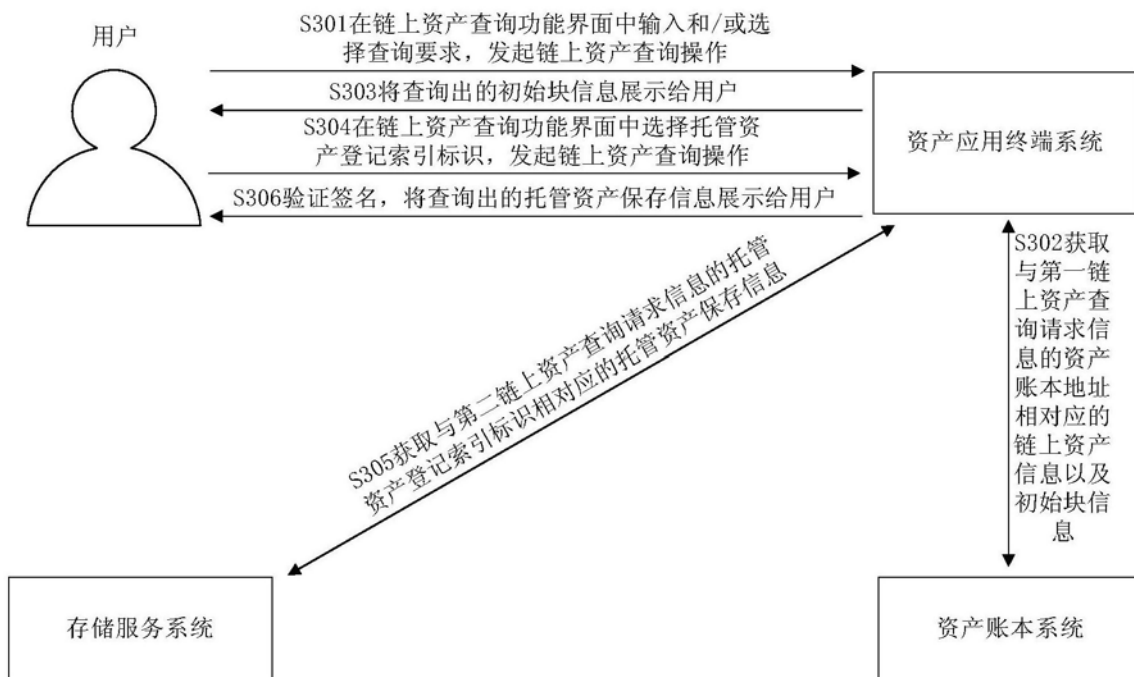


图3

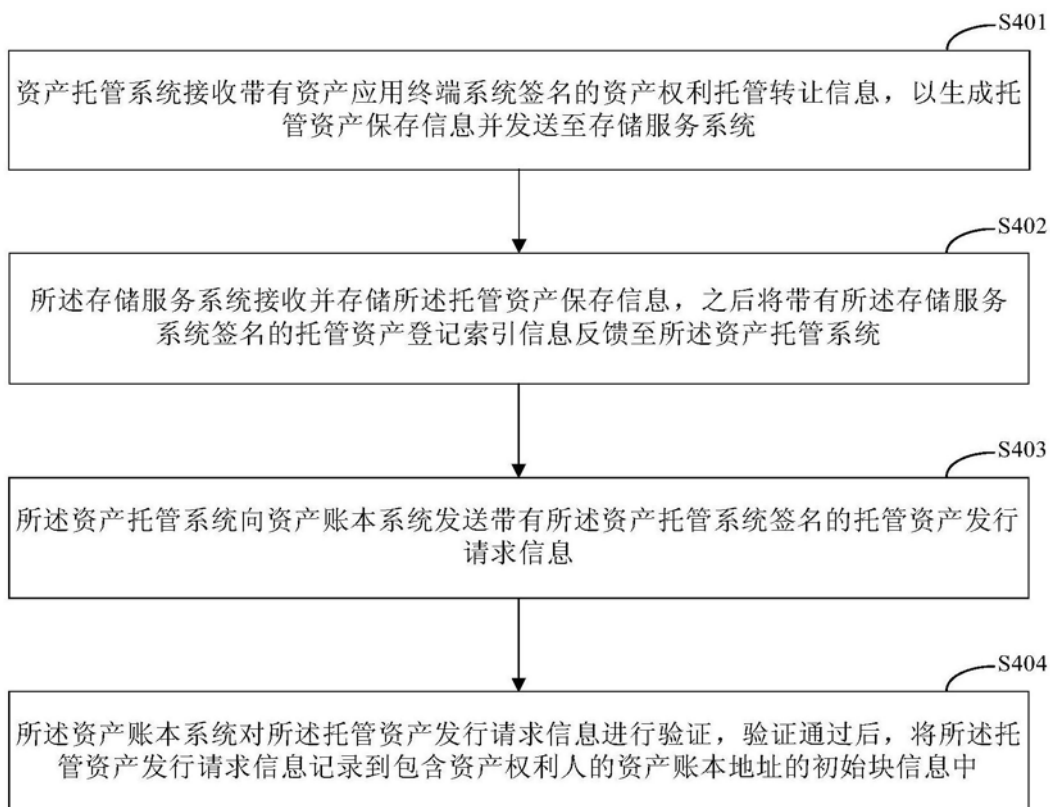


图4