(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113746638 B
(45)授权公告日 2023.04.07

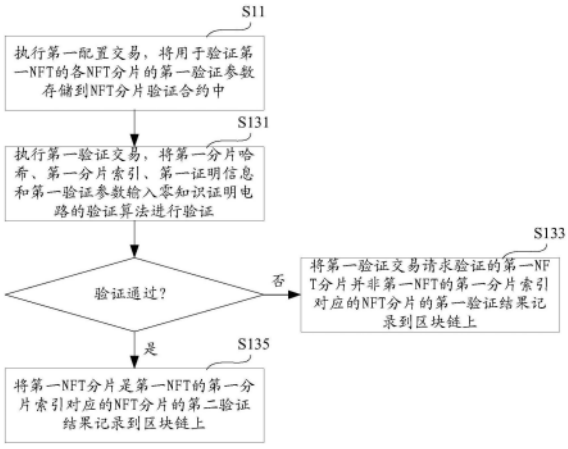
(21)申请号 202111033387.7
(22)申请日 2021.09.03
(65)同一申请的已公布的文献号
申请公布号 CN 113746638 A
(43)申请公布日 2021.12.03
(73)专利权人 杭州复杂美科技有限公司
地址 310000 浙江省杭州市西湖区文三路90号东部软件园6号楼7层702室
(72)发明人 马登极 王志文 吴思进
(51)Int.Cl.
H04L 9/32(2006.01)
G06F 16/27(2019.01)
G06F 16/22(2019.01)
(56)对比文件
CN 110300173 A,2019.10.01
CN 112968881 A,2021.06.15
审查员 王艳涛
权利要求书4页 说明书12页 附图5页

(54)发明名称

NFT存储方法、NFT还原方法、计算机设备和存储介质

(57)摘要

本发明提供一种NFT存储方法、NFT还原方法、计算机设备和存储介质，该方法包括：执行第一配置交易，将用于验证第一NFT的各NFT分片的第一验证参数存储到NFT分片验证合约中；执行第一验证交易，将第一验证交易提交的第一分片哈希、第一分片索引、第一证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：验证失败，则将第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；验证通过，则将第一NFT分片是第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上。本发明实现了降低NFT标记的数字资产的原始数据的泄露风险，同时在无需公开原始数据的前提下可以在区块链上验证数据。



CN 113746638 B

1.一种NFT存储方法,其特征在于,区块链部署有NFT分片验证合约,所述NFT分片验证合约配置有用于验证NFT分片的零知识证明电路,所述方法适用于区块链节点,所述方法包括:

执行第一配置交易,将用于验证第一NFT的各NFT分片的第一验证参数存储到所述NFT分片验证合约中;其中,所述第一验证参数由所述第一NFT的持有者的用户端将所述第一NFT对应的数字资产的原始数据生成若干个NFT分片、以各所述NFT分片的分片哈希作为叶子节点生成第一默克尔树之后,根据所述零知识证明电路的生成算法和所述第一默克尔树的树根所生成;

执行第一验证交易,将所述第一验证交易提交的第一分片哈希、第一分片索引、第一证明信息和所述第一验证参数输入所述零知识证明电路的验证算法进行验证:

验证失败,则将所述第一验证交易请求验证的第一NFT分片并非所述第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上;

验证通过,则将所述第一NFT分片是所述第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上;

其中,所述第一验证交易由第一存储服务端在收到所述用户端发送的第一NFT分片之后打包生成,所述第一分片哈希和所述第一分片索引分别为所述第一存储服务端所收到的第一NFT分片的分片哈希和分片索引;

所述第一证明信息由所述第一存储服务端以所述第一分片哈希、所述第一分片索引作为所述零知识证明电路的证明算法的公开输入,并以所述第一NFT分片、所述第一NFT分片在所述第一默克尔树中的第一默克尔路径作为所述证明算法的私密输入,所生成;

所述第一验证结果用于供所述第一存储服务端向所述用户端证明所接收的第一NFT分片有误并重新获取所述第一NFT分片;

所述第二验证结果用于供所述第一存储服务端确认所述第一NFT分片无误并存储。

2.一种NFT还原方法,其特征在于,第一NFT对应的数字资产的原始数据通过如权利要求1所述的NFT存储方法分片存储在若干个存储服务端中,所述NFT还原方法适用于区块链节点,所述NFT还原方法包括:

执行第二验证交易,将所述第二验证交易提交的第二分片哈希、第二分片索引、第二证明信息和所述第一验证参数输入所述零知识证明电路的验证算法进行验证:

验证失败,则将所述第二验证交易请求验证的第一NFT分片并非所述第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上;

验证通过,则将所述第一NFT分片是所述第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上;

其中,所述第二验证交易由所述用户端在收到所述第一存储服务端发回的第一NFT分片之后打包生成,所述第二分片哈希和所述第二分片索引分别为所述用户端所收到的所述第一存储服务端发回的第一NFT分片的分片哈希和分片索引;

所述第二证明信息由所述用户端以所述第二分片哈希、所述第二分片索引作为所述证明算法的公开输入,并以所述第一NFT分片、所述第一默克尔路径作为所述证明算法的私密输入,所生成;

所述第三验证结果用于供所述用户端向所述第一存储服务端证明所发回的第一NFT分

片有误；

所述第四验证结果用于供所述用户端确认所述第一NFT分片无误，并根据所述第一NFT分片和其它确认无误的NFT分片还原所述第一NFT对应的数字资产的原始数据。

3.一种NFT存储方法，其特征在于，区块链部署有NFT分片验证合约，所述NFT分片验证合约配置有用于验证NFT分片的零知识证明电路，所述方法适用于用户端，所述方法包括：

根据第一NFT对应的数字资产的原始数据生成若干个NFT分片；以各所述NFT分片的分片哈希作为叶子节点生成第一默克尔树；

根据所述零知识证明电路的生成算法和所述第一默克尔树的树根生成第一验证参数；

打包生成包括所述第一验证参数的第一配置交易并发送至区块链网络，以供区块链节点执行，将所述第一验证参数存储到所述NFT分片验证合约中；

分别将每个所述NFT分片发送给至少一个存储服务端，以供收到第一NFT分片的第一存储服务端：

以所收到的第一NFT分片的第一分片哈希、所收到的第一NFT分片的第一分片索引作为所述零知识证明电路的证明算法的公开输入，并以所述第一NFT分片、所述第一NFT分片在所述第一默克尔树中的第一默克尔路径作为所述证明算法的私密输入，生成第一证明信息；以及，

打包生成包括所述第一分片哈希、所述第一分片索引和所述第一证明信息的第一验证交易并发送至区块链网络，以供区块链节点执行，将所述第一分片哈希、所述第一分片索引、所述第一证明信息和所述第一验证参数输入所述零知识证明电路的验证算法进行验证：

验证失败，则将所述第一验证交易请求验证的第一NFT分片并非所述第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；

验证通过，则将所述第一NFT分片是所述第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上；

其中，所述第一验证结果用于供所述第一存储服务端向当前用户端证明所接收的第一NFT分片有误并重新获取所述第一NFT分片；

所述第二验证结果用于供所述第一存储服务端确认所述第一NFT分片无误并存储。

4.一种NFT还原方法，其特征在于，第一NFT对应的数字资产的原始数据通过如权利要求3所述的NFT存储方法分片存储在若干个存储服务端中，所述NFT还原方法适用于用户端，所述NFT还原方法包括：

分别向存储各所述NFT分片的各存储服务端发送NFT分片下载请求；

响应于接收到所述第一存储服务端发回的第一NFT分片，以所接收的第一NFT分片的第二分片哈希、所接收的第一NFT分片的第二分片索引作为所述证明算法的公开输入，并以所接收的第一NFT分片、所述第一默克尔路径作为所述证明算法的私密输入，生成第二证明信息；

打包生成包括所述第二分片哈希、所述第二分片索引、所述第二证明信息的第二验证交易并发送至区块链网络，以供区块链节点执行，将所述第二分片哈希、所述第二分片索引、所述第二证明信息和所述第一验证参数输入所述验证算法进行验证：

验证失败，则将所述第二验证交易请求验证的第一NFT分片并非所述第一NFT的第二分

片索引对应的NFT分片的第三验证结果记录到区块链上；

验证通过，则将所述第一NFT分片是所述第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上；

响应于获取到所述第三验证结果，向所述第一存储服务端证明所发回的第一NFT分片有误，重新向所述第一存储服务端或另一存储服务端下载所述第一NFT分片；

响应于获取到所述第四验证结果，根据所述第一NFT分片和其它确认无误的NFT分片还原所述第一NFT对应的数字资产的原始数据。

5.一种NFT存储方法，其特征在于，区块链部署有NFT分片验证合约，所述NFT分片验证合约配置有用于验证NFT分片的零知识证明电路，所述方法适用于存储服务端，所述方法包括：

响应于收到第一用户端发送的第一NFT分片，以所收到的第一NFT分片的第一分片哈希、所收到的第一NFT分片的第一分片索引作为所述零知识证明电路的证明算法的公开输入，并以所述第一NFT分片、所述第一NFT分片对应的第一默克尔路径作为所述证明算法的私密输入，生成第一证明信息；

打包生成包括所述第一分片哈希、所述第一分片索引和所述第一证明信息的第一验证交易并发送至区块链网络，以供区块链节点执行，将所述第一分片哈希、所述第一分片索引、所述第一证明信息和第一验证参数输入所述零知识证明电路的验证算法进行验证：

验证失败，则将所述第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；

验证通过，则将所述第一NFT分片是所述第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上；

响应于获取到所述第一验证结果，向所述用户端证明所接收的第一NFT分片有误并重新获取所述第一NFT分片；

响应于获取到所述第二验证结果，确认所述第一NFT分片无误并存储；

其中，所述第一验证参数由所述第一NFT的持有者的用户端将所述第一NFT对应的数字资产的原始数据生成若干个NFT分片、以各所述NFT分片的分片哈希作为叶子节点生成第一默克尔树之后，根据所述零知识证明电路的生成算法和所述第一默克尔树的树根所生成，并通过配置交易存储到所述NFT分片验证合约中。

6.一种NFT还原方法，其特征在于，第一NFT对应的数字资产的原始数据通过如权利要求5所述的NFT存储方法分片存储在若干个存储服务端中，所述NFT还原方法适用于存储服务端，所述NFT还原方法包括：

响应于接收到所述第一用户端发送的NFT分片下载请求，将所述第一NFT分片发送至所述第一用户端，以供所述第一用户端：

以所接收的第一NFT分片的第二分片哈希、所接收的第一NFT分片的第二分片索引作为所述证明算法的公开输入，并以所接收的第一NFT分片、所述第一默克尔路径作为所述证明算法的私密输入，生成第二证明信息；以及，

打包生成包括所述第二分片哈希、所述第二分片索引、所述第二证明信息的第二验证交易并发送至区块链网络，以供区块链节点执行，将所述第二分片哈希、所述第二分片索引、所述第二证明信息和所述第一验证参数输入所述验证算法进行验证：

验证失败,则将所述第二验证交易请求验证的第一NFT分片并非所述第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上;

验证通过,则将所述第一NFT分片是所述第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上;

其中,所述第三验证结果用于供所述第一用户端向当前存储服务端证明所发回的第一NFT分片有误;

所述第四验证结果用于供所述第一用户端根据所述第一NFT分片和其它确认无误的NFT分片还原所述第一NFT对应的数字资产的原始数据。

7.一种计算机设备,其特征在于,所述设备包括:

一个或多个处理器;

存储器,用于存储一个或多个程序,

当所述一个或多个程序被所述一个或多个处理器执行时,使得所述一个或多个处理器执行如权利要求1-6中任一项所述的方法。

8.一种存储有计算机程序的存储介质,其特征在于,该程序被处理器执行时实现如权利要求1-6中任一项所述的方法。

NFT存储方法、NFT还原方法、计算机设备和存储介质

技术领域

[0001] 本申请涉及区块链技术领域，具体涉及一种NFT存储方法、NFT还原方法、计算机设备和存储介质。

背景技术

[0002] NFT的英文全称为Non-Fungible Token，即，非同质化代币，具有不可分割、不可替代、独一无二等特点。

[0003] 相对应地，同质化代币即每个代币完全相同的代币，例如，一个游戏币和另一个游戏币，两者完全相同，没有任何区别；

[0004] 当前NFT的应用方式在于，每一个独一无二的NFT可以作为一份独一无二的数字资产的所有权标记，例如，NFT_1作为一个数字头像的所有权标记，NFT_2作为某游戏中一只虚拟猫的所有权标记，等等。

[0005] 上述方案的问题在于，当一个NFT所标记的数字资产是一种需要保密的数字资产时，例如，菜谱、配方、商业秘密等，NFT的所有者如果将数字资产的原始数据存储在本地，则会面临各类被线上或线下窃取的风险，而如果将数字资产的原始数据存储在各类存储服务器，则缺乏在不公开原始数据的前提下在区块链上验证数据的手段。例如，用户甲将某数字资产的原始数据的一个分片存储在服务器A，在用户甲需要还原数字资产时，却无法从服务器A获得正确的分片，此时双方可能各执一词，服务器A认为用户甲一开始就存储了错误的数据，用户甲则认为服务器A丢失了他的数据。

发明内容

[0006] 鉴于现有技术中的上述缺陷或不足，期望提供一种降低NFT标记的数字资产的原始数据的泄露风险，同时在无需公开原始数据的前提下可以在区块链上验证数据的NFT存储方法、NFT还原方法、计算机设备和存储介质。

[0007] 第一方面，本发明提供一种适用于区块链节点的NFT存储方法，区块链部署有NFT分片验证合约，NFT分片验证合约配置有用于验证NFT分片的零知识证明电路，该方法包括：

[0008] 执行第一配置交易，将用于验证第一NFT的各NFT分片的第一验证参数存储到NFT分片验证合约中；其中，第一验证参数由第一NFT的持有者的用户端将第一NFT对应的数字资产的原始数据生成若干个NFT分片、以各NFT分片的分片哈希作为叶子节点生成第一默克尔树之后，根据零知识证明电路的生成算法和第一默克尔树的树根所生成；

[0009] 执行第一验证交易，将第一验证交易提交的第一分片哈希、第一分片索引、第一证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：

[0010] 验证失败，则将第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；

[0011] 验证通过，则将第一NFT分片是第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上。

[0012] 其中，第一验证交易由第一存储服务端在收到用户端发送的第一NFT分片之后打包生成，第一分片哈希和第一分片索引分别为第一存储服务端所收到的第一NFT分片的分片哈希和分片索引；

[0013] 第一证明信息由第一存储服务端以第一分片哈希、第一分片索引作为零知识证明电路的证明算法的公开输入，并以第一NFT分片、第一NFT分片在第一默克尔树中的第一默克尔路径作为证明算法的私密输入，所生成；

[0014] 第一验证结果用于供第一存储服务端向用户端证明所接收的第一NFT分片有误并重新获取第一NFT分片；

[0015] 第二验证结果用于供第一存储服务端确认第一NFT分片无误并存储。

[0016] 第二方面，本发明提供一种适用于区块链节点的NFT还原方法，第一NFT对应的数字资产的原始数据通过如第一方面的NFT存储方法分片存储在若干个存储服务端中，该方法包括：

[0017] 执行第二验证交易，将第二验证交易提交的第二分片哈希、第二分片索引、第二证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：

[0018] 验证失败，则将第二验证交易请求验证的第一NFT分片并非第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上；

[0019] 验证通过，则将第一NFT分片是第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上。

[0020] 其中，第二验证交易由用户端在收到第一存储服务端发回的第一NFT分片之后打包生成，第二分片哈希和第二分片索引分别为用户端所收到的第一存储服务端发回的第一NFT分片的分片哈希和分片索引；

[0021] 第二证明信息由用户端以第二分片哈希、第二分片索引作为证明算法的公开输入，并以第一NFT分片、第一默克尔路径作为证明算法的私密输入，所生成；

[0022] 第三验证结果用于供用户端向第一存储服务端证明所发回的第一NFT分片有误；

[0023] 第四验证结果用于供用户端确认第一NFT分片无误，并根据第一NFT分片和其它确认无误的NFT分片还原第一NFT对应的数字资产的原始数据。

[0024] 第三方面，本发明还提供一种适用于用户端的NFT存储方法，区块链部署有NFT分片验证合约，NFT分片验证合约配置有用于验证NFT分片的零知识证明电路，该方法包括：

[0025] 根据第一NFT对应的数字资产的原始数据生成若干个NFT分片；

[0026] 以各NFT分片的分片哈希作为叶子节点生成第一默克尔树；

[0027] 根据零知识证明电路的生成算法和第一默克尔树的树根生成第一验证参数；

[0028] 打包生成包括第一验证参数的第一配置交易并发送至区块链网络，以供区块链节点执行，将第一验证参数存储到NFT分片验证合约中；

[0029] 分别将每个NFT分片发送给至少一个存储服务端，以供收到第一NFT分片的第一存储服务端：

[0030] 以所收到的第一NFT分片的第一分片哈希、所收到的第一NFT分片的第一分片索引作为零知识证明电路的证明算法的公开输入，并以第一NFT分片、第一NFT分片在第一默克尔树中的第一默克尔路径作为证明算法的私密输入，生成第一证明信息；以及，

[0031] 打包生成包括第一分片哈希、第一分片索引和第一证明信息的第一验证交易并发

送至区块链网络，以供区块链节点执行，将第一分片哈希、第一分片索引、第一证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：

[0032] 验证失败，则将第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；

[0033] 验证通过，则将第一NFT分片是第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上。

[0034] 其中，第一验证结果用于供第一存储服务端向当前用户端证明所接收的第一NFT分片有误并重新获取第一NFT分片；

[0035] 第二验证结果用于供第一存储服务端确认第一NFT分片无误并存储。

[0036] 第四方面，本发明还提供一种适用于用户端的NFT还原方法，第一NFT对应的数字资产的原始数据通过如第三方面的NFT存储方法分片存储在若干个存储服务端中，该方法包括：

[0037] 分别向存储各NFT分片的各存储服务端发送NFT分片下载请求；

[0038] 响应于接收到第一存储服务端发回的第一NFT分片，以所接收的第一NFT分片的第二分片哈希、所接收的第一NFT分片的第二分片索引作为证明算法的公开输入，并以所接收的第一NFT分片、第一默克尔路径作为证明算法的私密输入，生成第二证明信息；

[0039] 打包生成包括第二分片哈希、第二分片索引、第二证明信息的第二验证交易并发送至区块链网络，以供区块链节点执行，将第二分片哈希、第二分片索引、第二证明信息和第一验证参数输入验证算法进行验证：

[0040] 验证失败，则将第二验证交易请求验证的第一NFT分片并非第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上；

[0041] 验证通过，则将第一NFT分片是第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上；

[0042] 响应于获取到第三验证结果，向第一存储服务端证明所发回的第一NFT分片有误，重新向第一存储服务端或另一存储服务端下载第一NFT分片；

[0043] 响应于获取到第四验证结果，根据第一NFT分片和其它确认无误的NFT分片还原第一NFT对应的数字资产的原始数据。

[0044] 第五方面，本发明还提供一种适用于存储服务端的NFT存储方法，区块链部署有NFT分片验证合约，NFT分片验证合约配置有用于验证NFT分片的零知识证明电路，该方法包括：

[0045] 响应于收到第一用户端发送的第一NFT分片，以所收到的第一NFT分片的第一分片哈希、所收到的第一NFT分片的第一分片索引作为零知识证明电路的证明算法的公开输入，并以第一NFT分片、第一NFT分片对应的第一默克尔路径作为证明算法的私密输入，生成第一证明信息；

[0046] 打包生成包括第一分片哈希、第一分片索引和第一证明信息的第一验证交易并发送至区块链网络，以供区块链节点执行，将第一分片哈希、第一分片索引、第一证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：

[0047] 验证失败，则将第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；

[0048] 验证通过,则将第一NFT分片是第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上;

[0049] 响应于获取到第一验证结果,向用户端证明所接收的第一NFT分片有误并重新获取第一NFT分片;

[0050] 响应于获取到第二验证结果,确认第一NFT分片无误并存储。

[0051] 其中,第一验证参数由第一NFT的持有者的用户端将第一NFT对应的数字资产的原始数据生成若干个NFT分片、以各NFT分片的分片哈希作为叶子节点生成第一默克尔树之后,根据零知识证明电路的生成算法和第一默克尔树的树根所生成,并通过配置交易存储到NFT分片验证合约中。

[0052] 第六方面,本发明还提供一种适用于存储服务端的NFT还原方法,第一NFT对应的数字资产的原始数据通过如第五方面的NFT存储方法分片存储在若干个存储服务端中,该方法包括:

[0053] 响应于接收到第一用户端发送的NFT分片下载请求,将第一NFT分片发送至第一用户端,以供第一用户端:

[0054] 以所接收的第一NFT分片的第二分片哈希、所接收的第一NFT分片的第二分片索引作为证明算法的公开输入,并以所接收的第一NFT分片、第一默克尔路径作为证明算法的私密输入,生成第二证明信息;以及,

[0055] 打包生成包括第二分片哈希、第二分片索引、第二证明信息的第二验证交易并发送至区块链网络,以供区块链节点执行,将第二分片哈希、第二分片索引、第二证明信息和第一验证参数输入验证算法进行验证:

[0056] 验证失败,则将第二验证交易请求验证的第一NFT分片并非第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上;

[0057] 验证通过,则将第一NFT分片是第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上。

[0058] 其中,第三验证结果用于供第一用户端向当前存储服务端证明所发回的第一NFT分片有误;

[0059] 第四验证结果用于供第一用户端根据第一NFT分片和其它确认无误的NFT分片还原第一NFT对应的数字资产的原始数据。

[0060] 第七方面,本发明还提供一种计算机设备,包括一个或多个处理器和存储器,其中存储器包含可由该一个或多个处理器执行的指令以使得该一个或多个处理器执行根据本发明各实施例提供的方法。

[0061] 第八方面,本发明还提供一种存储有计算机程序的存储介质,该计算机程序使计算机执行根据本发明各实施例提供的方法。

[0062] 本发明诸多实施例提供的NFT存储方法、NFT还原方法、计算机设备和存储介质通过在智能合约中部署用于验证NFT分片的零知识证明电路,并将以各NFT分片的分片哈希作为叶子节点所生成的默克尔树的树根所生成的验证参数配置到上述智能合约中,使得存储服务器/用户端都可以在无需公开原始数据的前提下通过智能合约验证待存储的/所存储的数据是否有误,最终实现了降低NFT标记的数字资产的原始数据的泄露风险,同时在无需公开原始数据的前提下可以在区块链上验证数据。

附图说明

[0063] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0064] 图1为本发明一实施例提供的一种适用于区块链节点的NFT存储方法的流程图。

[0065] 图2为本发明一实施例提供的一种适用于区块链节点的NFT还原方法的流程图。

[0066] 图3为本发明一实施例提供的一种适用于用户端的NFT存储方法的流程图。

[0067] 图4为本发明一实施例提供的一种适用于用户端的NFT还原方法的流程图。

[0068] 图5为本发明一实施例提供的一种适用于存储服务端的NFT存储方法的流程图。

[0069] 图6为本发明一实施例提供的一种适用于存储服务端的NFT还原方法的流程图。

[0070] 图7为本发明一实施例提供的一种计算机设备的结构示意图。

具体实施方式

[0071] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与发明相关的部分。

[0072] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0073] 图1为本发明一实施例提供的一种适用于区块链节点的NFT存储方法的流程图。

[0074] 如图1所示，在本实施例中，本发明提供一种适用于区块链节点的NFT存储方法，包括：

[0075] S11：执行第一配置交易，将用于验证第一NFT的各NFT分片的第一验证参数存储到NFT分片验证合约中；其中，第一验证参数由第一NFT的持有者的用户端将第一NFT对应的数字资产的原始数据生成若干个NFT分片、以各NFT分片的分片哈希作为叶子节点生成第一默克尔树之后，根据零知识证明电路的生成算法和第一默克尔树的树根所生成；

[0076] S131：执行第一验证交易，将第一验证交易提交的第一分片哈希、第一分片索引、第一证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：

[0077] 验证失败，则执行步骤S133：将第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；

[0078] 验证通过，则执行步骤S135：将第一NFT分片是第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上。

[0079] 其中，第一验证交易由第一存储服务端在收到用户端发送的第一NFT分片之后打包生成，第一分片哈希和第一分片索引分别为第一存储服务端所收到的第一NFT分片的分片哈希和分片索引；

[0080] 第一证明信息由第一存储服务端以第一分片哈希、第一分片索引作为零知识证明电路的证明算法的公开输入，并以第一NFT分片、第一NFT分片在第一默克尔树中的第一默克尔路径作为证明算法的私密输入，所生成；

[0081] 第一验证结果用于供第一存储服务端向用户端证明所接收的第一NFT分片有误并重新获取第一NFT分片；

[0082] 第二验证结果用于供第一存储服务端确认第一NFT分片无误并存储。

[0083] 在本申请中，零知识证明电路基于以下原理进行验证：

[0084] 1、NFT分片的哈希值＝＝分片哈希；

[0085] 2、分片哈希*NFT分片对应的默克尔路径＝＝默克尔树根；

[0086] 3、分片索引与默克尔路径应当对应(每个分片哈希的默克尔路径是各不相同的)。

[0087] 本领域技术人员可以理解在零知识证明体系中如何根据上述验证原理生成零知识证明电路，所生成的零知识证明电路包括生成算法Setup()、证明算法Prove()和验证算法Verify()。具体过程此处不再赘述。

[0088] 以下以用户乙持有NFT_3，NFT_3用于标记一份需要保密的配方A，用户乙通过图1所示的方法存储配方A的原始数据为例，对图1所示的方法进行示例性的阐述。

[0089] 用户乙的用户端先根据配方A的原始数据$data_A$生成若干个NFT分片，例如，16个NFT分片$data_{A1}$-$data_{A16}$；

[0090] 在将上述16个NFT分片分别存储到若干个存储服务器之前，需要先对NFT分片验证合约进行验证参数的配置：

[0091] 以各NFT分片$data_{A1}$-$data_{A16}$的分片哈希$hash(data_{A1})$-$hash(data_{A16})$作为叶子节点，生成第一默克尔树；

[0092] 根据零知识证明电路的生成算法Setup()和第一默克尔树的树根$root_1$生成第一验证参数ver_key_1：

[0093] $Setup(root_1)\rightarrow ver\_key_1$；

[0094] 打包生成包括第一验证参数ver_key_1的第一配置交易tx1并发送至区块链网络。

[0095] 在步骤S11中，区块链节点通过NFT分片验证合约执行tx1，将用于验证NFT_3的各NFT分片的第一验证参数ver_key_1存储到NFT分片验证合约中。

[0096] 优选地，区块链节点在执行tx1时可以验证tx1的发送账户是否NFT_3的持有者：否，则不存储第一验证参数ver_key_1。

[0097] 完成验证参数的配置之后，用户乙的用户端将16个NFT分片$data_{A1}$-$data_{A16}$分别存储到若干个存储服务器(最好每个NFT分片都存储到多个存储服务器中)。

[0098] 以NFT分片$data_{A1}$存储到存储服务器B为例：

[0099] 用户乙的用户端将NFT分片$data_{A1}$及其分片哈希$hash(data_{A1})$、分片索引$index_1$、默克尔路径$merkle_path_1$发送至存储服务器B。其中，分片哈希也可以无需发送，由存储服务器B自行生成。

[0100] 存储服务器B收到上述信息后，以第一分片哈希$hash(data_{A1})$、第一分片索引$index_1$作为零知识证明电路的证明算法Prove()的公开输入，并以第一NFT分片$data_{A1}$、第一NFT分片在第一默克尔树中的第一默克尔路径$merkle_path_1$作为证明算法Prove()的私密输入，生成第一证明信息$prove_1$：

[0101] $Prove(hash(data_{A1})、index_1,data_{A1}、merkle\_path_1)\rightarrow prove_1$；

[0102] 然后再打包生成包括第一分片哈希$hash(data_{A1})$、第一分片索引$index_1$和第一证明信息$prove_1$的第一验证交易tx2并发送至区块链网络。

[0103] 在步骤S131中，区块链节点通过NFT分片验证合约执行tx2，将tx2提交的第一分片哈希$hash(data_{A1})$、第一分片索引$index_1$和第一证明信息$prove_1$，以及，tx2请求验证的NFT分片$data_{A1}$所对应的NFT_3所对应的验证参数ver_key_1输入零知识证明电路的验证算法

Verify()进行验证：

[0104] Verify(hash($data_{A1}$)、$index_1$,$prove_1$,ver_key_1)→Yes/No；

[0105] 当验证算法Verify()的输出结果为No时，验证失败，执行步骤S133：将tx2请求验证的NFT分片并非NFT_3的第$index_1$个NFT分片的第一验证结果记录到区块链上；

[0106] 当验证算法Verify()的输出结果为Yes时，验证通过，执行步骤S135：将tx2请求验证的NFT分片是NFT_3的第$index_1$个NFT分片的第二验证结果记录到区块链上。

[0107] 当存储服务器B从区块链上获取到上述第一验证结果时，存储服务器B根据tx2的执行结果向用户乙的用户端证明其所发送的NFT分片有误，并重新向用户乙的用户端获取$data_{A1}$等数据；

[0108] 当存储服务器B从区块链上获取到上述第二验证结果时，存储服务器B确认用户乙的用户端所发送的数据无误，存储$data_{A1}$等数据(具体可以加密存储或以本领域常用的其它方式存储)。

[0109] 将NFT分片$data_{A1}$存储到其它存储服务器，或，将其它NFT分片存储到若干个存储服务器的过程与上述NFT分片$data_{A1}$存储到存储服务器B的过程相同，不再一一赘述。

[0110] 优选地，用户乙还可以随时向任一存储服务器发起挑战，例如，挑战存储服务器B是否按照约定存储了NFT分片$data_{A1}$，此时存储服务器B同样可以通过打包生成一笔验证交易并发送至区块链网络的方式来证明自己履行了约定的存储义务。该验证交易的生成过程和执行过程与上述tx2的生成过程和执行过程完全相同，不再重复赘述。

[0111] 上述实施例通过在智能合约中部署用于验证NFT分片的零知识证明电路，并将以各NFT分片的分片哈希作为叶子节点所生成的默克尔树的树根所生成的验证参数配置到上述智能合约中，使得存储服务器可以在无需公开原始数据的前提下通过智能合约验证待存储的数据是否有误，最终实现了降低NFT标记的数字资产的原始数据的泄露风险，同时在无需公开原始数据的前提下可以在区块链上验证数据。

[0112] 图2为本发明一实施例提供的一种适用于区块链节点的NFT还原方法的流程图。如图2所示，在本实施例中，本发明还提供了一种适用于区块链节点的NFT还原方法，第一NFT对应的数字资产的原始数据通过如图1所示的NFT存储方法分片存储在若干个存储服务端中，该方法包括：

[0113] S211：执行第二验证交易，将第二验证交易提交的第二分片哈希、第二分片索引、第二证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：

[0114] 验证失败，则执行步骤S213：将第二验证交易请求验证的第一NFT分片并非第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上；

[0115] 验证通过，则执行步骤S215：将第一NFT分片是第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上。

[0116] 其中，第二验证交易由用户端在收到第一存储服务端发回的第一NFT分片之后打包生成，第二分片哈希和第二分片索引分别为用户端所收到的第一存储服务端发回的第一NFT分片的分片哈希和分片索引；

[0117] 第二证明信息由用户端以第二分片哈希、第二分片索引作为证明算法的公开输入，并以第一NFT分片、第一默克尔路径作为证明算法的私密输入，所生成；

[0118] 第三验证结果用于供用户端向第一存储服务端证明所发回的第一NFT分片有误；

[0119] 第四验证结果用于供用户端确认第一NFT分片无误，并根据第一NFT分片和其它确认无误的NFT分片还原第一NFT对应的数字资产的原始数据。

[0120] 具体地，同样以用户乙的用户端将NFT_3对应的配方A的原始数据$data_A$分割成16个NFT分片$data_{A1}$-$data_{A16}$，并将每个NFT分片存储到多个存储服务器为例，以下以用户乙的用户端还原NFT_3对应的$data_A$为例，对图2所示的方法进行示例性的阐述。

[0121] 在需要还原$data_A$时，用户乙的用户端分别向各存储服务端发送NFT分片下载请求。本领域技术人员可以理解，当多个存储服务器存有同一个NFT分片时，例如，存储服务器B和存储服务器C都存有$data_{A1}$时，此时可以只向其中一个存储服务器发送NFT分片下载请求。

[0122] 以用户乙的用户端向存储服务端B发送下载$data_{A1}$的NFT分片下载请求为例：

[0123] 存储服务端B在验证用户乙是NFT_3的持有者后(本领域技术人员可以理解相关的验证过程，具体不再展开)，将NFT分片$data_{A1}$及其分片哈希$hash(data_{A1})$、分片索引$index_1$、默克尔路径$merkle_path_1$发送给用户乙的用户端。具体地，本实施例以分片存储后用户乙的用户端不存储任何数据为例，在另一些实施例中，用户乙的用户端在分片存储后可以保留分片索引和默克尔路径等数据，则存储服务端此时可以只发送NFT分片$data_{A1}$。

[0124] 用户乙的用户端收到上述信息后，以第二分片哈希$hash(data_{A1})$、第二分片索引$index_1$作为零知识证明电路的证明算法Prove()的公开输入，并以第一NFT分片$data_{A1}$、第一默克尔路径$merkle_path_1$作为证明算法Prove()的私密输入，生成第二证明信息$prove_2$：

[0125] $Prove(hash(data_{A1})、index_1, data_{A1}、merkle\_path_1)\rightarrow prove_2$；

[0126] 然后再打包生成包括第二分片哈希$hash(data_{A1})$、第二分片索引$index_1$和第二证明信息$prove_2$的第一验证交易tx3并发送至区块链网络。

[0127] 在步骤S211中，区块链节点通过NFT分片验证合约执行tx3，将tx3提交的第二分片哈希$hash(data_{A1})$、第二分片索引$index_1$和第二证明信息$prove_2$，以及，tx3请求验证的NFT分片$data_{A1}$所对应的NFT_3所对应的验证参数ver_key_1输入零知识证明电路的验证算法Verify()进行验证：

[0128] $Verify(hash(data_{A1})、index_1, prove_2, ver\_key_1)\rightarrow Yes/No$；

[0129] 当验证算法Verify()的输出结果为No时，验证失败，执行步骤S213：将tx3请求验证的NFT分片并非NFT_3的第$index_1$个NFT分片的第三验证结果记录到区块链上；

[0130] 当验证算法Verify()的输出结果为Yes时，验证通过，执行步骤S215：将tx3请求验证的NFT分片是NFT_3的第$index_1$个NFT分片的第四验证结果记录到区块链上。

[0131] 当用户乙的用户端从区块链上获取到上述第三验证结果时，用户乙的用户端根据tx3的执行结果向存储服务端B证明下载的NFT分片有误，重新向存储服务端B下载$data_{A1}$，或，向另一存储服务端C下载$data_{A1}$；

[0132] 当用户乙的用户端从区块链上获取到上述第四验证结果时，用户乙的用户端确认从存储服务端B下载的$data_{A1}$无误，并最终在确认下载的16个NFT分片$data_{A1}$-$data_{A16}$全部无误后，根据$data_{A1}$-$data_{A16}$还原NFT_3对应的配方A的原始数据$data_A$。

[0133] 上述实施例通过在智能合约中部署用于验证NFT分片的零知识证明电路，并将以各NFT分片的分片哈希作为叶子节点所生成的默克尔树的树根所生成的验证参数配置到上述智能合约中，使得用户端可以在无需公开原始数据的前提下通过智能合约验证存储服务

器所存储的数据是否有误，最终实现了降低NFT标记的数字资产的原始数据的泄露风险，同时在无需公开原始数据的前提下可以在区块链上验证数据。

[0134] 图3为本发明一实施例提供的一种适用于用户端的NFT存储方法的流程图。图3所示的方法可配合图1所示的方法执行。

[0135] 如图3所示，在本实施例中，本发明还提供一种适用于用户端的NFT存储方法，区块链部署有NFT分片验证合约，NFT分片验证合约配置有用于验证NFT分片的零知识证明电路，该方法包括：

[0136] S31：根据第一NFT对应的数字资产的原始数据生成若干个NFT分片；

[0137] S33：以各NFT分片的分片哈希作为叶子节点生成第一默克尔树；

[0138] S35：根据零知识证明电路的生成算法和第一默克尔树的树根生成第一验证参数；

[0139] S37：打包生成包括第一验证参数的第一配置交易并发送至区块链网络，以供区块链节点执行，将第一验证参数存储到NFT分片验证合约中；

[0140] S39：分别将每个NFT分片发送给至少一个存储服务端，以供收到第一NFT分片的第一存储服务端：

[0141] 以所收到的第一NFT分片的第一分片哈希、所收到的第一NFT分片的第一分片索引作为零知识证明电路的证明算法的公开输入，并以第一NFT分片、第一NFT分片在第一默克尔树中的第一默克尔路径作为证明算法的私密输入，生成第一证明信息；以及，

[0142] 打包生成包括第一分片哈希、第一分片索引和第一证明信息的第一验证交易并发送至区块链网络，以供区块链节点执行，将第一分片哈希、第一分片索引、第一证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：

[0143] 验证失败，则将第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；

[0144] 验证通过，则将第一NFT分片是第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上。

[0145] 其中，第一验证结果用于供第一存储服务端向当前用户端证明所接收的第一NFT分片有误并重新获取第一NFT分片；

[0146] 第二验证结果用于供第一存储服务端确认第一NFT分片无误并存储。

[0147] 图3所示方法的NFT存储原理可参照图1所示的方法，此处不再赘述。

[0148] 图4为本发明一实施例提供的一种适用于用户端的NFT还原方法的流程图。图4所示的方法可配合图2所示的方法执行。

[0149] 如图4所示，在本实施例中，本发明还提供一种适用于用户端的NFT还原方法，第一NFT对应的数字资产的原始数据通过如第三方面的NFT存储方法分片存储在若干个存储服务端中，该方法包括：

[0150] S41：分别向存储各NFT分片的各存储服务端发送NFT分片下载请求；

[0151] S43：响应于接收到第一存储服务端发回的第一NFT分片，以所接收的第一NFT分片的第二分片哈希、所接收的第一NFT分片的第二分片索引作为证明算法的公开输入，并以所接收的第一NFT分片、第一默克尔路径作为证明算法的私密输入，生成第二证明信息；

[0152] S45：打包生成包括第二分片哈希、第二分片索引、第二证明信息的第二验证交易并发送至区块链网络，以供区块链节点执行，将第二分片哈希、第二分片索引、第二证明信

息和第一验证参数输入验证算法进行验证：

[0153] 验证失败，则将第二验证交易请求验证的第一NFT分片并非第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上；

[0154] 验证通过，则将第一NFT分片是第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上；

[0155] 响应于获取到第三验证结果，执行步骤S47：向第一存储服务端证明所发回的第一NFT分片有误，重新向第一存储服务端或另一存储服务端下载第一NFT分片；

[0156] 响应于获取到第四验证结果，执行步骤S49：根据第一NFT分片和其它确认无误的NFT分片还原第一NFT对应的数字资产的原始数据。

[0157] 图4所示方法的NFT还原原理可参照图2所示的方法，此处不再赘述。

[0158] 图5为本发明一实施例提供的一种适用于存储服务端的NFT存储方法的流程图。图3所示的方法可配合图1、3所示的方法执行。

[0159] 如图5所示，在本实施例中，本发明还提供一种适用于存储服务端的NFT存储方法，区块链部署有NFT分片验证合约，NFT分片验证合约配置有用于验证NFT分片的零知识证明电路，该方法包括：

[0160] S51：响应于收到第一用户端发送的第一NFT分片，以所收到的第一NFT分片的第一分片哈希、所收到的第一NFT分片的第一分片索引作为零知识证明电路的证明算法的公开输入，并以第一NFT分片、第一NFT分片对应的第一默克尔路径作为证明算法的私密输入，生成第一证明信息；

[0161] S53：打包生成包括第一分片哈希、第一分片索引和第一证明信息的第一验证交易并发送至区块链网络，以供区块链节点执行，将第一分片哈希、第一分片索引、第一证明信息和第一验证参数输入零知识证明电路的验证算法进行验证：

[0162] 验证失败，则将第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上；

[0163] 验证通过，则将第一NFT分片是第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上；

[0164] 响应于获取到第一验证结果，执行步骤S55：向用户端证明所接收的第一NFT分片有误并重新获取第一NFT分片；

[0165] 响应于获取到第二验证结果，执行步骤S57：确认第一NFT分片无误并存储。

[0166] 其中，第一验证参数由第一NFT的持有者的用户端将第一NFT对应的数字资产的原始数据生成若干个NFT分片、以各NFT分片的分片哈希作为叶子节点生成第一默克尔树之后，根据零知识证明电路的生成算法和第一默克尔树的树根所生成，并通过配置交易存储到NFT分片验证合约中。

[0167] 图5所示方法的NFT还原原理同样可参照图1所示的方法，此处不再赘述。

[0168] 图6为本发明一实施例提供的一种适用于存储服务端的NFT还原方法的流程图。图6所示的方法可配合图2、4所示的方法执行。

[0169] 如图6所示，在本实施例中，本发明还提供一种适用于存储服务端的NFT还原方法，第一NFT对应的数字资产的原始数据通过如第五方面的NFT存储方法分片存储在若干个存储服务端中，该方法包括：

[0170] S61:响应于接收到第一用户端发送的NFT分片下载请求,将第一NFT分片发送至第一用户端,以供第一用户端:

[0171] 以所接收的第一NFT分片的第二分片哈希、所接收的第一NFT分片的第二分片索引作为证明算法的公开输入,并以所接收的第一NFT分片、第一默克尔路径作为证明算法的私密输入,生成第二证明信息;以及,

[0172] 打包生成包括第二分片哈希、第二分片索引、第二证明信息的第二验证交易并发送至区块链网络,以供区块链节点执行,将第二分片哈希、第二分片索引、第二证明信息和第一验证参数输入验证算法进行验证:

[0173] 验证失败,则将第二验证交易请求验证的第一NFT分片并非第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上;

[0174] 验证通过,则将第一NFT分片是第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上。

[0175] 其中,第三验证结果用于供第一用户端向当前存储服务端证明所发回的第一NFT分片有误;

[0176] 第四验证结果用于供第一用户端根据第一NFT分片和其它确认无误的NFT分片还原第一NFT对应的数字资产的原始数据。

[0177] 图6所示方法的NFT还原原理同样可参照图2所示的方法,此处不再赘述。

[0178] 图7为本发明一实施例提供的一种计算机设备的结构示意图。

[0179] 如图7所示,作为另一方面,本申请还提供了一种计算机设备700,包括一个或多个中央处理单元(CPU)701,其可以根据存储在只读存储器(ROM)702中的程序或者从存储部分708加载到随机访问存储器(RAM)703中的程序而执行各种适当的动作和处理。在RAM703中,还存储有设备700操作所需的各种程序和数据。CPU701、ROM702以及RAM703通过总线704彼此相连。输入/输出(I/O)接口705也连接至总线704。

[0180] 以下部件连接至I/O接口705:包括键盘、鼠标等的输入部分706;包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分707;包括硬盘等的存储部分708;以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分709。通信部分709经由诸如因特网的网络执行通信处理。驱动器710也根据需要连接至I/O接口705。可拆卸介质711,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器710上,以便于从其上读出的计算机程序根据需要被安装入存储部分708。

[0181] 特别地,根据本公开的实施例,上述任一实施例描述的方法可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括有形地包含在机器可读介质上的计算机程序,计算机程序包含用于执行上述任一方法的程序代码。在这样的实施例中,该计算机程序可以通过通信部分709从网络上被下载和安装,和/或从可拆卸介质711被安装。

[0182] 作为又一方面,本申请还提供了一种计算机可读存储介质,该计算机可读存储介质可以是上述实施例的装置中所包含的计算机可读存储介质;也可以是单独存在,未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序,该程序被一个或者一个以上的处理器用来执行描述于本申请提供的方法。

[0183] 附图中的流程图和框图,图示了按照本发明各种实施例的系统、方法和计算机程

序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这根据所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以通过执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以通过专用硬件与计算机指令的组合来实现。

[0184] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中，例如，各单元可以是设置在计算机或移动智能设备中的软件程序，也可以是单独配置的硬件装置。其中，这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0185] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本申请中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离本申请构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

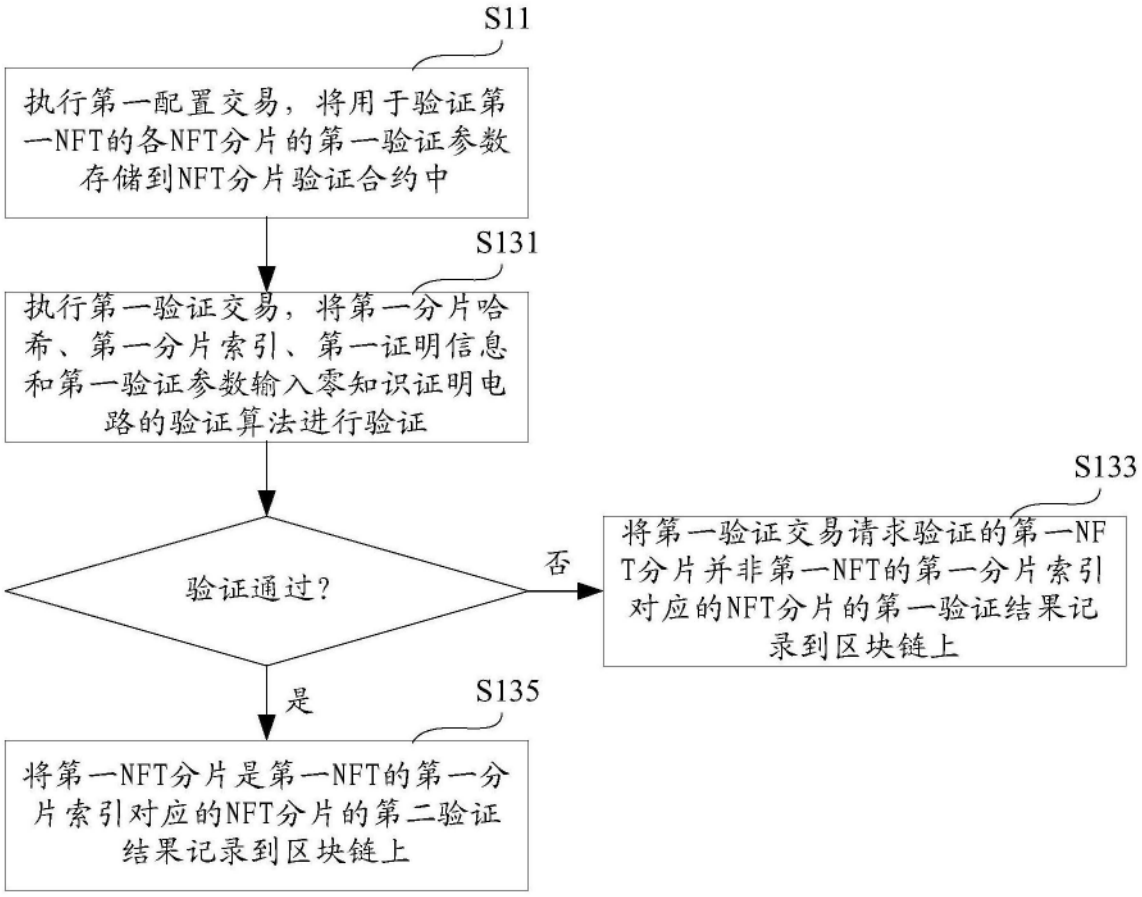

S11
执行第一配置交易，将用于验证第一NFT的各NFT分片的第一验证参数存储到NFT分片验证合约中
S131
执行第一验证交易，将第一分片哈希、第一分片索引、第一证明信息和第一验证参数输入零知识证明电路的验证算法进行验证
验证通过？
否
S133
将第一验证交易请求验证的第一NFT分片并非第一NFT的第一分片索引对应的NFT分片的第一验证结果记录到区块链上
是
S135
将第一NFT分片是第一NFT的第一分片索引对应的NFT分片的第二验证结果记录到区块链上

图1

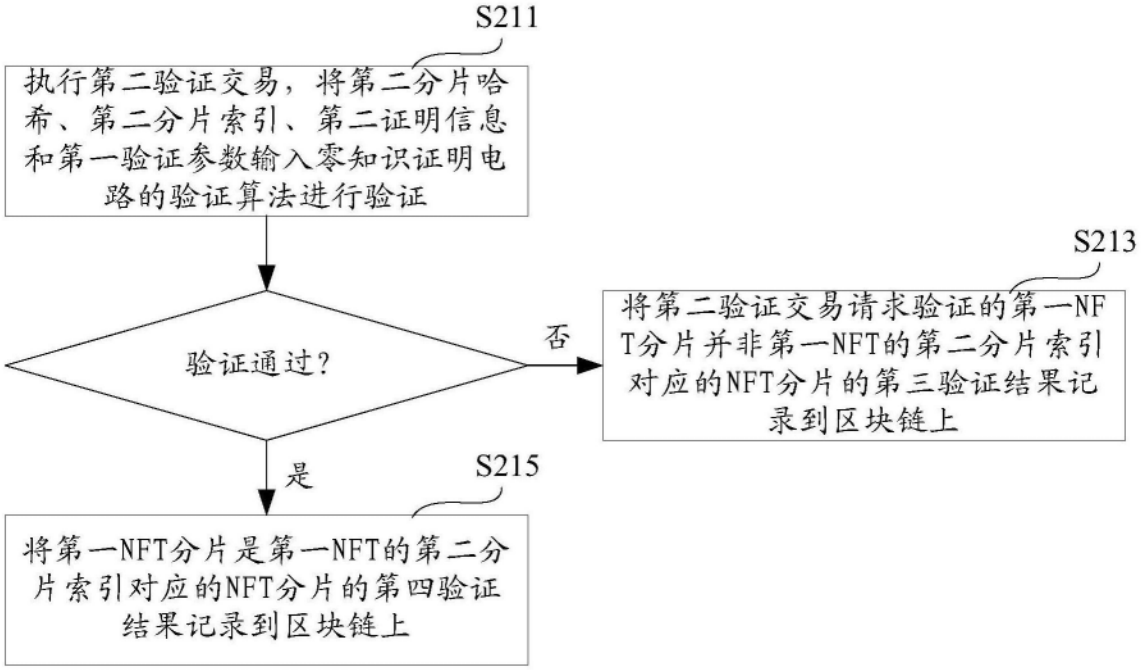

S211
执行第二验证交易，将第二分片哈希、第二分片索引、第二证明信息和第一验证参数输入零知识证明电路的验证算法进行验证
验证通过？
否
S213
将第二验证交易请求验证的第一NFT分片并非第一NFT的第二分片索引对应的NFT分片的第三验证结果记录到区块链上
是
S215
将第一NFT分片是第一NFT的第二分片索引对应的NFT分片的第四验证结果记录到区块链上

图2

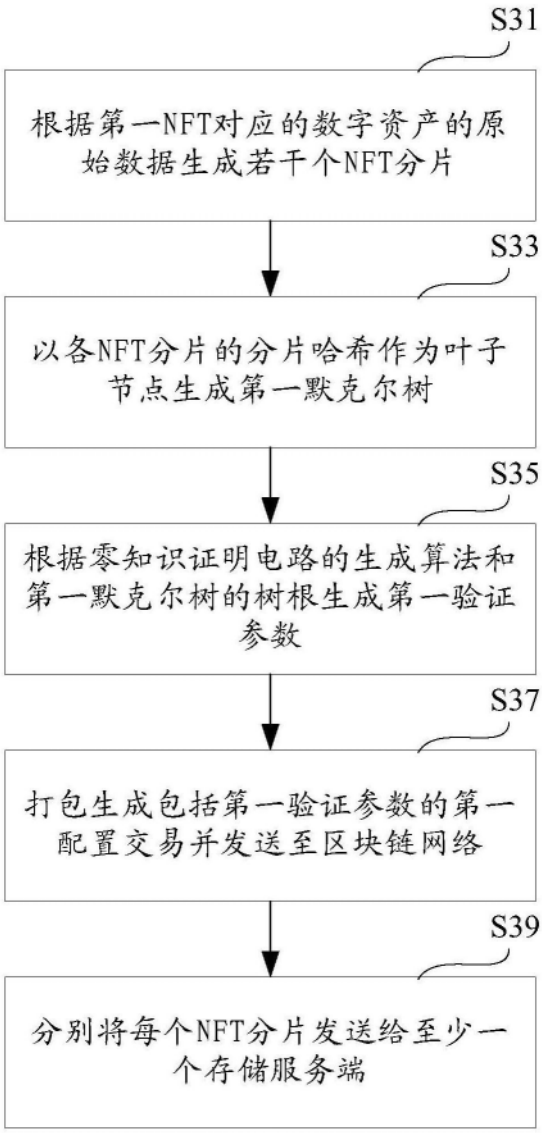

S31
根据第一NFT对应的数字资产的原始数据生成若干个NFT分片
S33
以各NFT分片的分片哈希作为叶子节点生成第一默克尔树
S35
根据零知识证明电路的生成算法和第一默克尔树的树根生成第一验证参数
S37
打包生成包括第一验证参数的第一配置交易并发送至区块链网络
S39
分别将每个NFT分片发送给至少一个存储服务端

图3

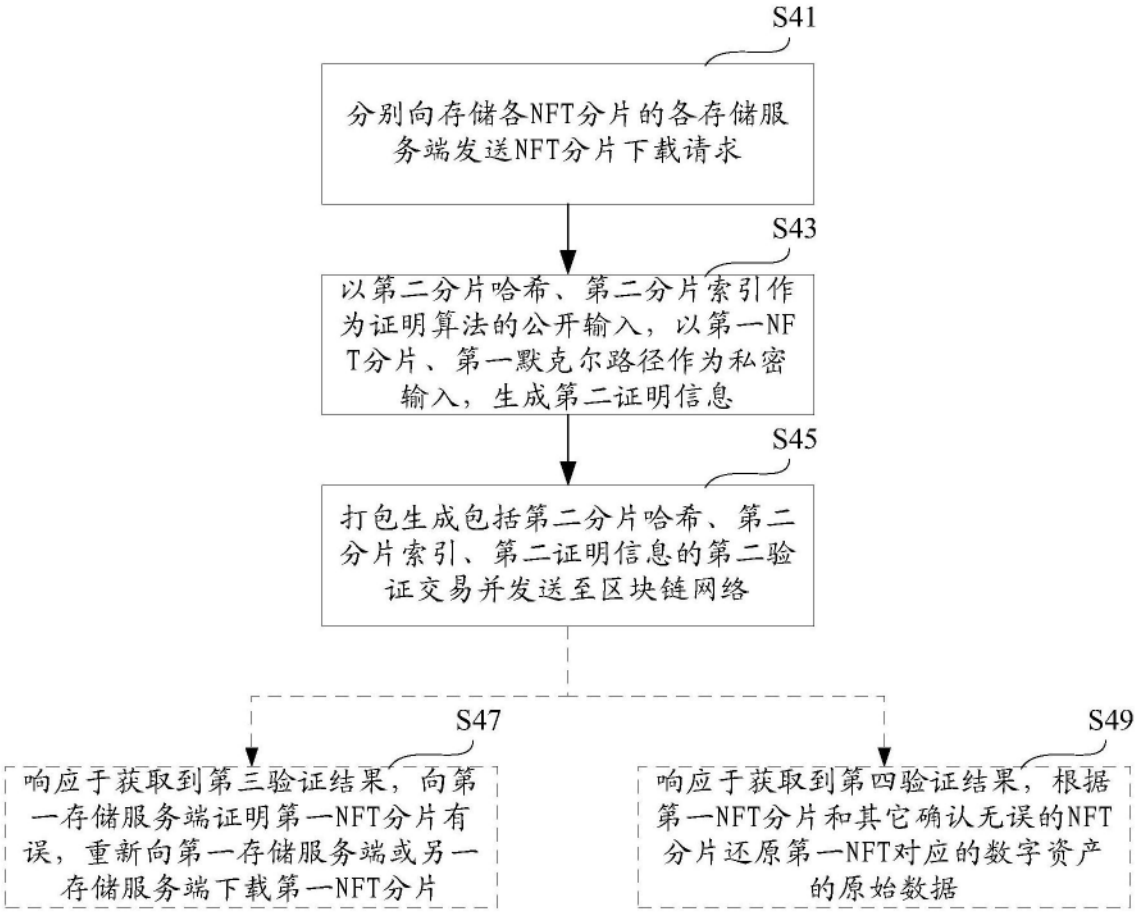

S41
分别向存储各NFT分片的各存储服务端发送NFT分片下载请求
S43
以第二分片哈希、第二分片索引作为证明算法的公开输入，以第一NFT分片、第一默克尔路径作为私密输入，生成第二证明信息
S45
打包生成包括第二分片哈希、第二分片索引、第二证明信息的第二验证交易并发送至区块链网络
S47
响应于获取到第三验证结果，向第一存储服务端证明第一NFT分片有误，重新向第一存储服务端或另一存储服务端下载第一NFT分片
S49
响应于获取到第四验证结果，根据第一NFT分片和其它确认无误的NFT分片还原第一NFT对应的数字资产的原始数据

图4

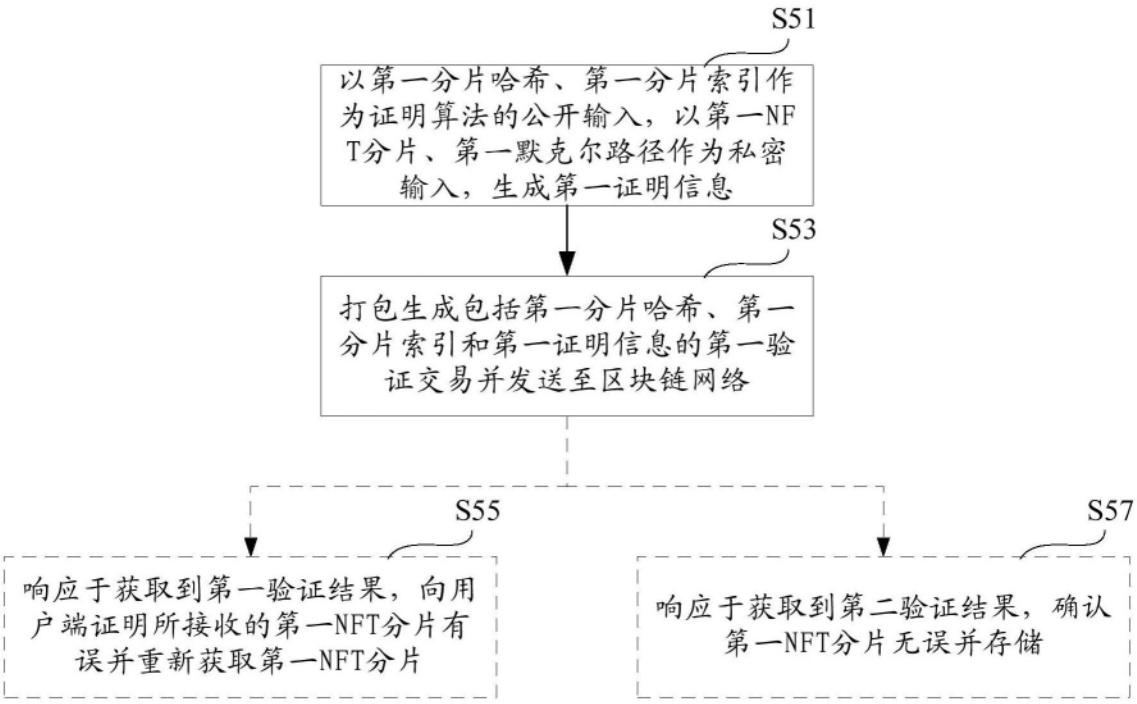

S51
以第一分片哈希、第一分片索引作为证明算法的公开输入，以第一NFT分片、第一默克尔路径作为私密输入，生成第一证明信息
S53
打包生成包括第一分片哈希、第一分片索引和第一证明信息的第一验证交易并发送至区块链网络
S55
响应于获取到第一验证结果，向用户端证明所接收的第一NFT分片有误并重新获取第一NFT分片
S57
响应于获取到第二验证结果，确认第一NFT分片无误并存储

图5

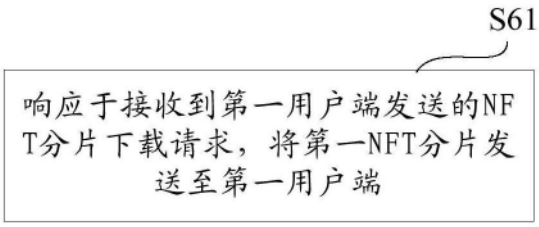

S61
响应于接收到第一用户端发送的NFT分片下载请求，将第一NFT分片发送至第一用户端

图6

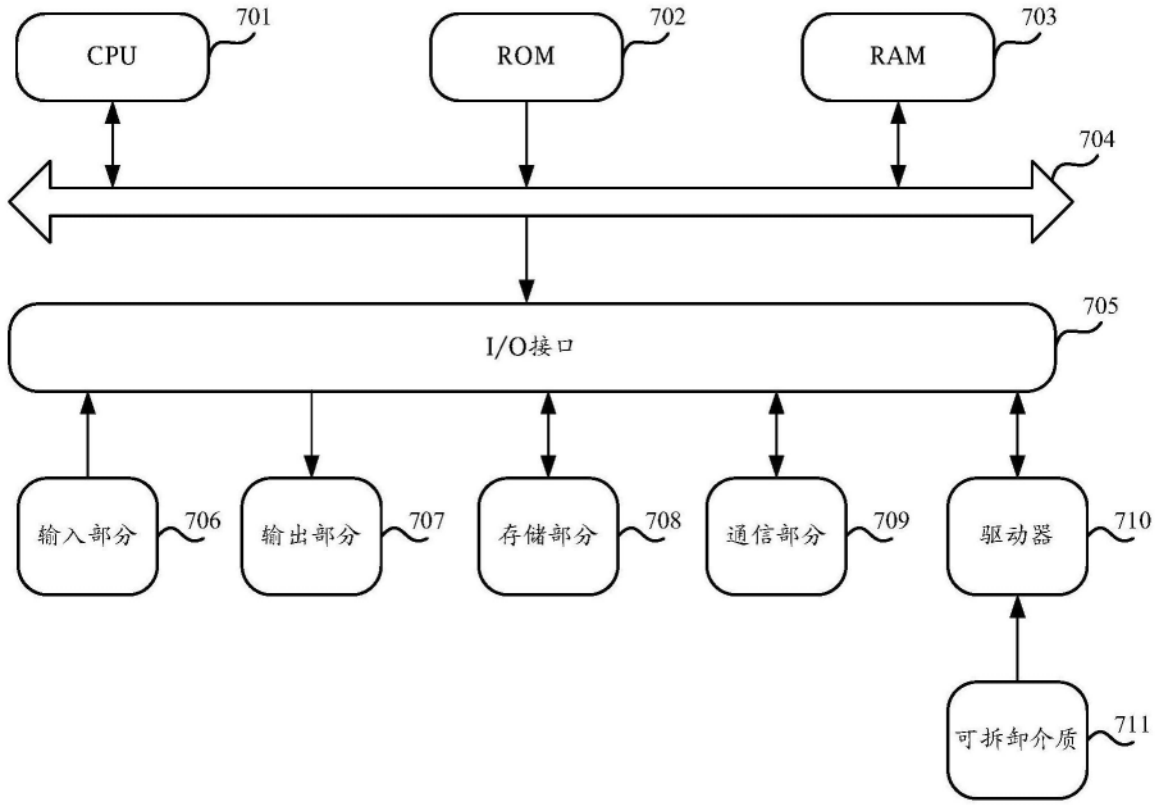

CPU
701
ROM
702
RAM
703
704
I/O接口
705
输入部分
706
输出部分
707
存储部分
708
通信部分
709
驱动器
710
可拆卸介质
711

图7