



(12) 发明专利

(10) 授权公告号 CN 114066456 B

(45) 授权公告日 2022.04.08

(21) 申请号 202210034457.9

(22) 申请日 2022.01.13

(65) 同一申请的已公布的文献号  
申请公布号 CN 114066456 A

(43) 申请公布日 2022.02.18

(73) 专利权人 环球数科集团有限公司  
地址 518063 广东省深圳市南山区粤海街  
道高新南九道10号深圳湾科技生态园  
10栋B座17层01-03号

(72) 发明人 张卫平 丁焯 米小武 李显阔  
岑全 张伟

(74) 专利代理机构 北京清控智云知识产权代理  
事务所(特殊普通合伙)  
11919

代理人 马肃

(51) Int.Cl.

G06F 17/11 (2006.01)

G06Q 20/38 (2012.01)

G06Q 40/04 (2012.01)

(56) 对比文件

CN 111639924 A, 2020.09.08

CN 101179486 A, 2008.05.14

CN 107667509 A, 2018.02.06

CN 110741372 A, 2020.01.31

CN 112232823 A, 2021.01.15

CN 112783853 A, 2021.05.11

WO 2018115567 A1, 2018.06.28

审查员 张榆

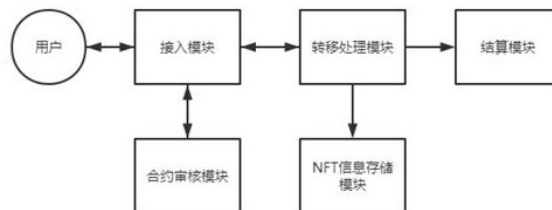
权利要求书2页 说明书6页 附图2页

(54) 发明名称

一种基于ERC1155的跨链NFT转移和结算系统

(57) 摘要

本发明提供了一种基于ERC1155的跨链NFT转移和结算系统,包括结算模块、接入模块、合约审核模块、NFT信息存储模块和转移处理模块,所述接入模块用于对接用户及其所在的链,所述合约审核模块用于审核用户所在链是否基于ERC1155合约,所述转移处理模块用于接收用户发送的NFT转移数据包并对所述NFT转移数据包进行处理,所述NFT信息存储模块用于保存NFT的存储信息地址,所述结算模块用于对完成的NFT转移作最终的结算记录;本系统能够实现NFT在不同的区块链中进行转移,在转移过程中不涉及NFT自身内容,仅仅是对NFT转移的合法性进行验证以及对记录NFT转移的区块地址进行记录,简化了流程而不弱化效果,提高NFT的转移效率。



1. 一种基于ERC1155的跨链NFT转移和结算系统,其特征在于,包括结算模块、接入模块、合约审核模块、NFT信息存储模块和转移处理模块,所述接入模块用于对接用户及其所在的链,所述合约审核模块用于审核用户所在链是否基于ERC1155合约,所述转移处理模块用于接收用户发送的NFT转移数据包并对所述NFT转移数据包进行处理,所述NFT信息存储模块用于保存NFT的存储信息地址,所述结算模块用于对完成的NFT转移作最终的结算记录;

所述转移处理模块对所述NFT转移数据包中的所有NFT信息进行验证,验证通过后向用户所在的链发送NFT转移信息,用户所在链根据所述NFT转移信息生成区块完成NFT转移,用户所在链生成的区块地址被发送至所述结算模块,所述结算模块对区块地址进行记录;

所述NFT转移数据包包括包头和包内容,所述包头用于配对和资源分配,具有相同包头的NFT转移数据包合成一个NFT交易包,所述包内容用于记录NFT信息;

所述包头数据包括四个数据段,第一数据段表示此次NFT转移涉及的用户数量,第二数据段表示此次NFT转移设计的NFT数量,第三数据段表示时间期限要求,第四数据段表示NFT转移双方的口令;

所述转移处理模块计算出NFT交易包的优先指数,所述优先指数Y的计算公式为:

$$Y = k \cdot (n2)^{n1} \cdot \left[ \frac{1}{\log_{t0}(n3 - T_{now})} \right];$$

其中,n1表示包头的第二数据段的值,n2表示包头的第三数据段的值,n3表示包头的第四数据段的值, $T_{now}$ 为当前时间对应的值,t0表示时间基数,k为调整系数;

所述转移处理模块对NFT信息进行验证需要的资源总数为 $N_z$ ,所述转移处理模块将资源总数依据优先指数进行分配,第i个交易包分配的资源数量 $N_i$ 为:

$$N_i = N_z \cdot \left( \frac{Y_i \cdot \text{Num}(Y_j < Y_i)}{n \cdot \sum_{j=1}^n Y_j} \right);$$

其中, $Y_i$ 表示第i个交易包的优先指数,n为现存的配对的交易包的数量, $\text{Num}(Y_j < Y_i)$ 表示优先指数小于 $Y_i$ 的交易包的数量。

2. 如权利要求1所述的一种基于ERC1155的跨链NFT转移和结算系统,其特征在于,所述NFT转移数据包的包内容包括若干条NFT信息条,每条NFT信息条包括NFT\_ID、NFT拥有者信息、NFT转移对象信息和NFT存储信息地址。

3. 如权利要求2所述的一种基于ERC1155的跨链NFT转移和结算系统,其特征在于,所述转移处理模块包括信息条处理单元、NFT存储验证单元、NFT拥有者验证单元和NFT转移输出单元,所述NFT存储验证单元从所述信息条处理单元中获取NFT存储信息地址并对对应的NFT内容进行验证,所述NFT拥有者验证单元从所述信息条处理单元中获取到以NFT拥有者信息分类的用户验证包并对用户是否拥有对应的NFT进行验证,所述转移处理模块的验证资源分配给所述NFT存储验证单元和NFT拥有者验证单元。

4. 如权利要求3所述的一种基于ERC1155的跨链NFT转移和结算系统,其特征在于,所述NFT转移输出单元从所述信息条处理单元中获取到以NFT转移对象信息分类的NFT接收包,

当所述NFT存储验证单元和NFT所有者验证单元对一个交易包中的所有NFT信息条验证完毕后,所述NFT转移输出单元将所述NFT接收包和用户验证包合并后发送至对应用户的区块链。

5. 如权利要求4所述的一种基于ERC1155的跨链NFT转移和结算系统,其特征在于,所述NFT信息存储模块还用于存储NFT的密钥,所述密钥用于访问NFT的存储地址,所述NFT信息存储模块在完成NFT的交易后对NFT的新所有者开放权限,NFT的新所有者在所述NFT信息存储模块中获取到NFT的存储地址以及密钥。

## 一种基于ERC1155的跨链NFT转移和结算系统

### 技术领域

[0001] 本公开大体上涉及NFT技术领域,且更明确地说涉及一种基于ERC1155的跨链NFT转移和结算系统。

### 背景技术

[0002] NFT指非同质化代币,用于表示数字资产的唯一加密货币令牌,可以买卖,目前大部分NFT是在基于ERC1155智能合约的区块链中证明其拥有者身份的,当NFT在不同的区块链中转移时,过程比较繁杂,而且效率较低,现在需要一种能够高效处理NFT转移的结算系统来加快NFT的流通性。

[0003] 现在已经开发出了很多NFT转移系统,经过大量的检索与参考,发现现有的转移系统有如公开号为KR101733599B1, KR101837169B1、CN111639924B和KR101826372B1所公开的系统,方法包括:将货物实体转化为token信息;在智能合约中创建四种协议;所述四种协议包括创建拍卖协议、支付担保协议、竞标协议和发货保证协议;通过创建拍卖协议创建卖家的拍卖实例,将token信息保存在区块链中,并采用发货保证协议锁定区块链中的token信息;将竞标者的资产实体存储在支付担保协议中作为保证金;在区块链中启动拍卖实例,采用竞标协议完成竞拍流程,并保存出价记录,将出价记录复制到区块链中每个节点上;竞标流程完成后,利用创建拍卖协议对卖家的账户进行付款,通过所述发货保证协议执行发货流程。但该系统主要用于处理NFT的拍卖,其本身设计的NFT数量不大,效率较低,不适合用于处理大规模的NFT转移。

### 发明内容

[0004] 本发明的目的在于,针对所存在的不足,提出了一种基于ERC1155的跨链NFT转移和结算系统。

[0005] 本发明采用如下技术方案:

[0006] 一种基于ERC1155的跨链NFT转移和结算系统,包括结算模块、接入模块、合约审核模块、NFT信息存储模块和转移处理模块,所述接入模块用于对接用户及其所在的链,所述合约审核模块用于审核用户所在链是否基于ERC1155合约,所述转移处理模块用于接收用户发送的NFT转移数据包并对所述NFT转移数据包进行处理,所述NFT信息存储模块用于保存NFT的存储信息地址,所述结算模块用于对完成的NFT转移作最终的结算记录;

[0007] 所述转移处理模块对所述NFT转移数据包中的所有NFT信息进行验证,验证通过后向用户所在的链发送NFT转移信息,用户所在链根据所述NFT转移信息生成区块完成NFT转移,用户所在链生成的区块地址被发送至所述结算模块,所述结算模块对区块地址进行记录;

[0008] 所述NFT转移数据包包括包头和包内容,所述包头用于配对和资源分配,具有相同包头的NFT转移数据包合成一个NFT交易包,所述包内容用于记录NFT信息;

[0009] 所述包头数据包括四个数据段,第一数据段表示此次NFT转移涉及的用户数量,第

二数据段表示此次NFT转移设计的NFT数量,第三数据段表示时间期限要求,第四数据段表示NFT转移双方的口令;

[0010] 所述转移处理模块计算出NFT交易包的优先指数,所述优先指数Y的计算公式为:

$$[0011] \quad Y = k \cdot (n2)^{n1} \cdot \left[ \frac{1}{\log_{t0}(n3 - T_{now})} \right];$$

[0012] 其中,n1表示包头的第二数据段的值,n2表示包头的第三数据段的值,n3表示包头的第四数据段的值, $T_{now}$ 为当前时间对应的值,t0表示时间基数,k为调整系数;

[0013] 所述转移处理模块对NFT信息进行验证需要的资源总数为 $N_z$ ,所述转移处理模块将资源总数依据优先指数进行分配,第i个交易包分配的资源数量 $N_i$ 为:

$$[0014] \quad N_i = N_z \cdot \left( \frac{Y_i \cdot \text{Num}(Y_j < Y_i)}{n \cdot \sum_{j=1}^n Y_j} \right);$$

[0015] 其中, $Y_i$ 表示第i个交易包的优先指数,n为现存的配对的交易包的数量, $\text{Num}(Y_j < Y_i)$ 表示优先指数小于 $Y_i$ 的交易包的数量;

[0016] 进一步的,所述NFT转移数据包的包内容包括若干条NFT信息条,每条NFT信息条包括NFT\_ID、NFT所有者信息、NFT转移对象信息和NFT存储信息地址;

[0017] 进一步的,所述转移处理模块包括信息条处理单元、NFT存储验证单元、NFT所有者验证单元和NFT转移输出单元,所述NFT存储验证单元从所述信息条处理单元中获取NFT存储信息地址并对对应的NFT内容进行验证,所述NFT所有者验证单元从所述信息条处理单元中获取到以NFT所有者信息分类的用户验证包并对用户是否拥有对应的NFT进行验证,所述转移处理模块的验证资源分配给所述NFT存储验证单元和NFT所有者验证单元;

[0018] 进一步的,所述NFT转移输出单元从所述信息条处理单元中获取到以NFT转移对象信息分类的NFT接收包,当所述NFT存储验证单元和NFT所有者验证单元对一个交易包中的所有NFT信息条验证完毕后,所述NFT转移输出单元将所述NFT接收包和用户验证包合并后发送至对应用户的区块链;

[0019] 进一步的,所述NFT信息存储模块还用于存储NFT的密钥,所述密钥用于访问NFT的存储地址,所述NFT信息存储模块在完成NFT的交易后对NFT的新所有者开放权限,NFT的新所有者在所述NFT信息存储模块中获取到NFT的存储地址以及密钥。

[0020] 本发明所取得的有益效果是:

[0021] 本系统不涉及对NFT内容本身的处理和对交易本身的记录,能够大大地减少非必要操作,为提高NFT的转移效率奠定基础,本系统主要是对NFT转移的合法性进行验证,验证过程中根据NFT的原所有者进行分类,使NFT能够批量进行验证,提高了验证的效率,本系统对NFT的转移请求进行优先度计算,根据优先度计算结果对验证的资源进行合理分配,使用户在提交转移请求后的总等待时间最优化,提高用户的体验。

[0022] 为使能更进一步了解本发明的特征及技术内容,请参阅以下有关本发明的详细说

明与附图,然而所提供的附图仅用于提供参考与说明,并非用来对本发明加以限制。

### 附图说明

- [0023] 图1为本发明整体结构框架示意图;  
 [0024] 图2为本发明NFT转移结算流程示意图;  
 [0025] 图3为本发明转移处理模块结构框架示意图;  
 [0026] 图4为本发明用户验证包分类示意图;  
 [0027] 图5为本发明NFT接收包分类示意图。

### 具体实施方式

[0028] 以下是通过特定的具体实施例来说明本发明的实施方式,本领域技术人员可由本说明书所公开的内容了解本发明的优点与效果。本发明可通过其他不同的具体实施例加以施行或应用,本说明书中的各项细节也可基于不同观点与应用,在不悖离本发明的精神下进行各种修饰与变更。另外,本发明的附图仅为简单示意说明,并非依实际尺寸的描绘,事先声明。以下的实施方式将进一步详细说明本发明的相关技术内容,但所公开的内容并非用以限制本发明的保护范围。

[0029] 实施例一。

[0030] 本实施例提供了一种基于ERC1155的跨链NFT转移和结算系统,结合图1,包括结算模块、接入模块、合约审核模块、NFT信息存储模块和转移处理模块,所述接入模块用于对接用户及其所在的链,所述合约审核模块用于审核用户所在链是否基于ERC1155合约,所述转移处理模块用于接收用户发送的NFT转移数据包并对所述NFT转移数据包进行处理,所述NFT信息存储模块用于保存NFT的存储信息地址,所述结算模块用于对完成的NFT转移作最终的结算记录;

[0031] 所述转移处理模块对所述NFT转移数据包中的所有NFT信息进行验证,验证通过后向用户所在的链发送NFT转移信息,用户所在链根据所述NFT转移信息生成区块完成NFT转移,用户所在链生成的区块地址被发送至所述结算模块,所述结算模块对区块地址进行记录;

[0032] 所述NFT转移数据包包括包头和包内容,所述包头用于配对和资源分配,具有相同包头的NFT转移数据包合成一个NFT交易包,所述包内容用于记录NFT信息;

[0033] 所述包头数据包括四个数据段,第一数据段表示此次NFT转移涉及的用户数量,第二数据段表示此次NFT转移设计的NFT数量,第三数据段表示时间期限要求,第四数据段表示NFT转移双方的口令;

[0034] 所述转移处理模块计算出NFT交易包的优先指数,所述优先指数Y的计算公式为:

$$[0035] \quad Y = k \cdot (n2)^{n1} \cdot \left[ \frac{1}{\log_{t0}(n3 - T_{now})} \right];$$

[0036] 其中,n1表示包头的第一个数据段的值,n2表示包头的第二个数据段的值,n3表示包头的第三个数据段的值, $T_{now}$ 为当前时间对应的值,t0表示时间基数,k为调整系数;

[0037] 所述转移处理模块对NFT信息进行验证需要的资源总数为Nz,所述转移处理模块

将资源总数依据优先指数进行分配,第*i*个交易包分配的资源数量 $N_i$ 为:

$$[0038] \quad N_i = N_z \cdot \left( \frac{Y_i \cdot \text{Num}(Y_j < Y_i)}{n \cdot \sum_{j=1}^n Y_j} \right);$$

[0039] 其中, $Y_i$ 表示第*i*个交易包的优先指数, $n$ 为现存的配对的交易包的数量, $\text{Num}(Y_j < Y_i)$ 表示优先指数小于 $Y_i$ 的交易包的数量;

[0040] 所述NFT转移数据包的包内容包括若干条NFT信息条,每条NFT信息条包括NFT\_ID、NFT所有者信息、NFT转移对象信息和NFT存储信息地址;

[0041] 所述转移处理模块包括信息条处理单元、NFT存储验证单元、NFT所有者验证单元和NFT转移输出单元,所述NFT存储验证单元从所述信息条处理单元中获取NFT存储信息地址并对对应的NFT内容进行验证,所述NFT所有者验证单元从所述信息条处理单元中获取到以NFT所有者信息分类的用户验证包并对用户是否拥有对应的NFT进行验证,所述转移处理模块的验证资源分配给所述NFT存储验证单元和NFT所有者验证单元;

[0042] 所述NFT转移输出单元从所述信息条处理单元中获取到以NFT转移对象信息分类的NFT接收包,当所述NFT存储验证单元和NFT所有者验证单元对一个交易包中的所有NFT信息条验证完毕后,所述NFT转移输出单元将所述NFT接收包和用户验证包合并后发送至对应用户的区块链;

[0043] 所述NFT信息存储模块还用于存储NFT的密钥,所述密钥用于访问NFT的存储地址,所述NFT信息存储模块在完成NFT的交易后对NFT的新所有者开放权限,NFT的新所有者在所述NFT信息存储模块中获取到NFT的存储地址以及密钥。

[0044] 实施例二。

[0045] 本实施例包含了实施例一的全部内容,提供了一种基于ERC1155的跨链NFT转移和结算系统,包括结算模块、接入模块、合约审核模块、NFT信息存储模块和转移处理模块,所述接入模块用于完成NFT转移双方所在链的对接,所述合约审核模块用于对接入链的合约进行审核,所述转移处理模块用于接收NFT转移请求并进行处理,所述NFT信息存储模块用于保存NFT的存储信息地址,所述结算模块用于记录NFT转移双方所在链上记录此次转移的区块的区块信息;

[0046] 结合图2,所述系统进行NFT转移和结算的过程包括如下步骤:

[0047] S1、NFT转移双方所在链与所述接入模块进行对接;

[0048] S2、NFT转移双方向所述系统提交智能合约副本;

[0049] S3、所述合约审核模块对所述智能合约副本进行校对,判断是否为ERC1155合约,若符合,则返回审核通过信息,若不符合,则返回审核不通过信息,并通知所述接入模块与审核不通过的NFT转移方断开连接;

[0050] S4、合约通过审核后,所述NFT转移双方向所述系统发送NFT转移数据包;

[0051] S5、所述转移处理模块根据所述NFT转移数据包的包头进行配对,配对的NFT转移数据包合成一个NFT交易包;

[0052] S6、所述转移处理模块对NFT交易包中的所有NFT进行信息验证,当所有NFT信息验

证通过后,将NFT的存储信息地址发送至所述NFT信息存储模块进行保存,同时向NFT转移双方所在链发送NFT转移信息;

[0053] S7、NFT转移双方所在链根据接收到的NFT转移信息生成区块进行记录,并将生成区块的区块地址发送至所述结算模块;

[0054] S8、所述结算模块根据接收到的区块地址访问对应的区块,确认区块内容符合NFT转移内容后,在所述结算模块上的结算链上生成结算区块,所述结算区块用于记录接收到的NFT双方所在链生成的区块的区块地址信息;

[0055] 所述NFT转移数据包包括包头和包内容,所述包内容包括若干条NFT信息条,所述NFT交易包由信息条构成,所述NFT信息条中的内容包括NFT\_ID、NFT所有者信息、NFT转移对象信息和NFT存储信息地址;

[0056] 所述NFT转移数据包的包头为一串数据,该数据包括四个数据段,第一数据段表示此次NFT转移涉及的用户数量,第二数据段表示此次NFT转移设计的NFT数量,第三数据段表示时间期限要求,第四数据段表示NFT转移双方的口令,所述数据段之间用短线分隔连接;

[0057] 当系统要同时处理大量的NFT转移时,所述转移处理模块根据包头的三个数据段计算出对应的NFT交易包的优先指数,所述转移处理模块依据优先指数分配相应的资源数量进行NFT的转移处理;

[0058] 所述优先指数Y的计算公式为:

$$[0059] \quad Y = k \cdot (n2)^{n1} \cdot \left[ \frac{1}{\log_{t0}(n3 - T_{now})} \right];$$

[0060] 其中,n1表示包头的第二数据段的值,n2表示包头的第三数据段的值,n3表示包头的第四数据段的值, $T_{now}$ 为当前时间对应的值,t0表示时间基数,k为调整系数;

[0061] 需要注意的是,用于在设置包头的第四数据段时,n3会远大于当前时刻,若n3接近或小于当前时刻,所述转移处理模块会退回NFT转移数据包;

[0062] 所述转移处理单元的资源数量总量为 $N_z$ ,配对后的现存第i个NFT交易包的优先指数用 $Y_i$ 表示,则第i个NFT交易包分配得到的资源数量为:

$$[0063] \quad N_i = N_z \cdot \left( \frac{Y_i \cdot \text{Num}(Y_j < Y_i)}{n \cdot \sum_{j=1}^n Y_j} \right);$$

[0064] 其中,n为现存的配对的交易包的数量, $\text{Num}(Y_j < Y_i)$ 表示优先指数小于 $Y_i$ 的交易包的数量;

[0065] 需要注意的是,通过上述过程计算的所有交易包分配得到的资源数量之和小于 $N_z$ ,缺少的部分资源数量用于应急处理;

[0066] 结合图3、图4和图5,所述转移处理模块包括信息条处理单元、NFT存储验证单元、NFT所有者验证单元和NFT转移输出单元,所述信息条处理单元从所述NFT交易包中逐条获取NFT信息条,进行三项处理,第一项处理为根据所述NFT所有者信息进行分类,得到若干个用户验证包,每个用户验证包中包括一个NFT所有者信息和若干个NFT\_ID,所述用户验证包



发送至所述NFT拥有者验证单元,第二项处理为将NFT存储信息地址发送至所述NFT存储验证单元,所述NFT存储验证单元实时地对每个NFT的存储地址进行验证,第三项处理为根据所述NFT转移对象信息进行分类,得到若干个NFT接收包,每个NFT接收包中包括一个NFT转移对象信息和若干个NFT\_ID,所述NFT接收包发送至所述NFT转移输出单元;

[0067] 所述NFT存储验证单元访问接收到的每一个NFT存储信息地址,确认每一个地址存有对应NFT的内容后,向所述NFT转移输出单元发送NFT存储验证成功指令;

[0068] 所述NFT拥有者验证单元根据用户验证包中的NFT拥有者信息到对应的区块链中获取其所有的NFT信息,并与所述用户验证包中的每个NFT\_ID进行核对,确认其拥有所有的NFT并且没有转出记录,当所述NFT拥有者验证单元完成所有用户验证包的验证后,向所述NFT转移输出单元发送NFT拥有者验证成功指令以及所有的用户验证包;

[0069] 所述NFT转移输出单元在接收到NFT存储验证成功指令和NFT拥有者验证成功指令后,将所述NFT接收包和用户验证包进行合并与格式转换,合并指当NFT接收包中的NFT转移对象信息与用户验证包中的NFT拥有者信息为同一用户时,将这两个包合并,格式转换指将包中的NFT\_ID转换成具体的转入/转出信息描述,格式转换后的包称为NFT转移输出包,所述NFT转移输出单元根据所述NFT转移输出包中的用户信息发送至对应的区块链;

[0070] 上述过程完成了NFT的所有权的转移,下面对NFT的访问权的转移进行说明;

[0071] 所述NFT的实际内容保存在第三方的存储空间中,所述第三方的存储空间地址为NFT存储信息地址,在完成NFT的转移前,仅有NFT的所有者拥有访问NFT实际内容的密钥,在转移过程中,NFT的拥有者会向所述NFT存储验证单元发送一次性密钥,所述NFT存储验证单元通过所述一次性密钥访问对应NFT内容完成验证;

[0072] 在步骤S8中,当所述结算模块在完成对区块内容的确认后,以及生成结算区块前,所述结算模块向所有NFT的原拥有者获取访问NFT实际内容的密钥,对所有密钥进行更改后将新密钥保存在所述NFT信息存储模块中,在所述NFT信息存储模块,新密钥与NFT的存储信息地址配对保存且设置有独立的访问权限,所述结算模块在生成结算区块后,对NFT的新拥有者开放对应的NFT信息存储模块访问权限,NFT的新拥有者在所述NFT信息存储模块中获取新密钥以及NFT的存储信息地址。

[0073] 以上所公开的内容仅为本发明的优选可行实施例,并非因此局限本发明的保护范围,所以凡是运用本发明说明书及附图内容所做的等效技术变化,均包含于本发明的保护范围内,此外,随着技术发展其中的元素可以更新的。

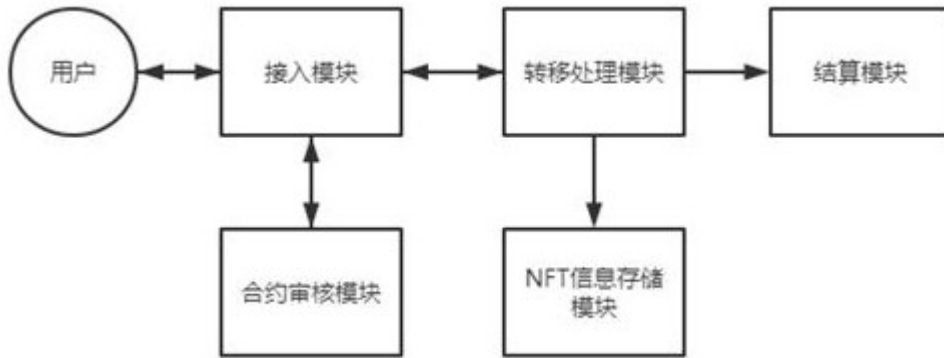


图1

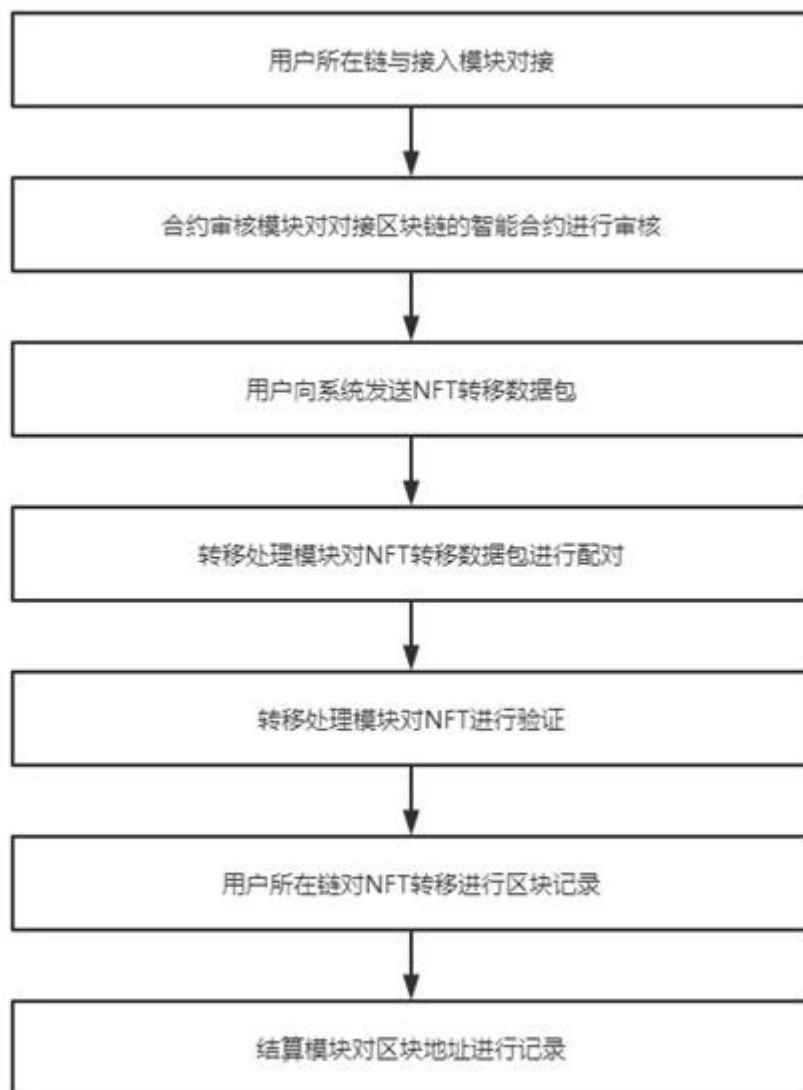


图2

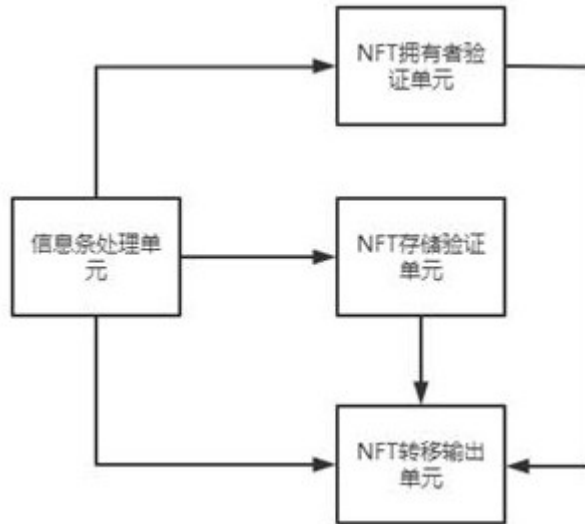


图3

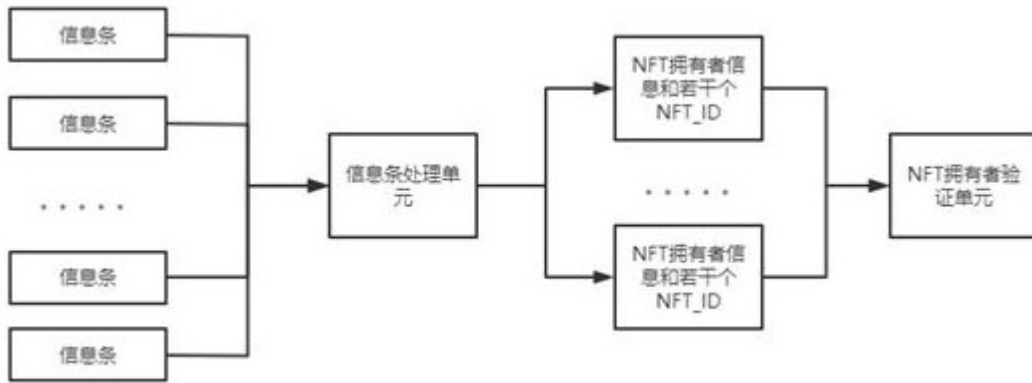


图4

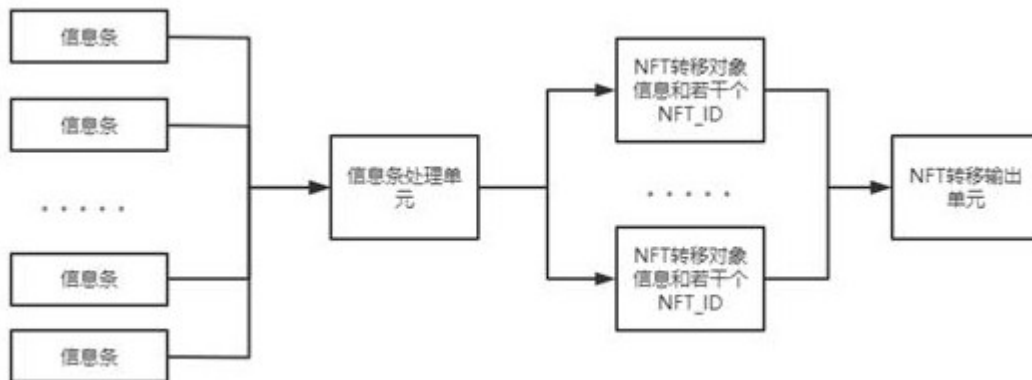


图5