(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 107945021 A
(43)申请公布日 2018.04.20

(21)申请号 201711285268.4

(22)申请日 2017.12.07

(71)申请人 杭州趣链科技有限公司
地址 310012 浙江省杭州市西湖区文三路199号13幢南楼501室

(72)发明人 李启雷 李伟 梁秀波 邱炜伟 尹可挺

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 邱启旺

(51)Int.Cl.
G06Q 40/04(2012.01)
G06Q 20/38(2012.01)

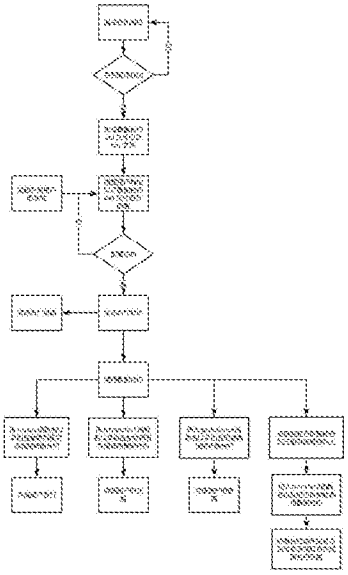
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种基于区块链智能合约的数字资产管理方法

(57)摘要

本发明公开了一种基于区块链智能合约的数字资产管理方法，该方法是在基于智能合约的区块链网络上，发起交易的一方可以通过部署智能合约来创建资产，调用智能合约来发行资产以及交易资产、查询资产。本发明实现了利用基于区块链智能合约的数字资产管理方法完成创建资产、发行资产、合约内交易资产、跨合约交易资产和查询资产，利用区块链数据不可篡改的特点实现了交易的安全性以及可靠性。



CN 107945021 A

1.一种基于区块链智能合约的数字资产管理方法，其特征在于，该方法包括如下步骤：

(1)编译合约源代码，获取源代码对应的智能合约bin、智能合约的abi和发起交易的用户地址；

(2)通过步骤(1)中获得的智能合约bin、发起交易的用户地址进行智能合约部署，获得智能合约地址，完成资产的创建；

(3)根据所述的发起交易的用户传入的方法名以及相应的参数列表，实现获取payload；

(4)当要发行资产时，通过步骤(1)获取的发起交易的用户地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload来调用智能合约中的函数来完成；

当要在智能合约内进行资产的交易、查询时，通过步骤(1)获取的发起交易的用户地址、获取交易的用户的地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload调用智能合约中的函数来完成。

当要进行跨合约交易时，首先将交易发起方的智能合约注册到统筹合约上，然后通过步骤(1)获取的发起交易的用户地址、获取交易的用户的地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload来调用智能合约中的跨合约交易函数，最后由统筹合约调用交易方法来与交易获取方完成跨合约交易。

2.根据权利要求1所述的基于区块链智能合约的数字资产管理，其特征在于，所述的资产的发行需调用智能合约中的issue函数以及相应的参数列表。

3.根据权利要求1所述的基于区块链智能合约的数字资产管理方法，其特征在于，所述的资产的交易需调用智能合约中的transfer1函数以及相应的参数列表。

4.根据权利要求1所述的基于区块链智能合约的数字资产管理方法，其特征在于，所述的资产的查询需调用智能合约中的getBalance函数以及相应的参数列表。

5.根据权利要求1所述的基于区块链智能合约的数字资产管理方法，其特征在于，所述的跨合约交易需调用智能合约中的transfer2函数以及相应的参数列表。

一种基于区块链智能合约的数字资产管理方法

技术领域

[0001] 本发明涉及区块链技术和智能合约，尤其涉及一种基于区块链智能合约的数字资产管理方法。

背景技术

[0002] 目前的资产交易方式有两种：传统的资产交易和初始代币交易(ICO)。传统的资产交易：此过程需要相应的中间商，如资产所有者证明、真实性公证等均需第三方介入才能完成，只有通过资产发行方、资产接收方、交易平台等多方介入，资产才可以完成整个交易。此模式存在的痛点：(1)资产进入交易后，必须依赖资产发行方才能完成使用、转移，这就将资产交易范围限制在了发行方系统的用户群内；(2)资产交易依赖于有限的行业大渠道，而近乎垄断的渠道费用导致交易成本大幅提高，同时小渠道及个体投资者难以在资产流通环节发挥其应有的作用。

[0003] 初始代币交易(ICO)：ICO本质上是一种共享经济或共同致富模式，是让没有专业技能的小规模投资者能够获得一些项目早期投资收益的机会，也是让达不到融资门槛的创业者通过分享利润获得项目资金的一种方式。但是，目前ICO代币的交易价格会受到人为因素影响，或仅靠买卖价格进行交易，而与企业的数字资产无关，这使得ICO的社会公信力不够高，甚至为不法欺诈行为埋下隐患。

发明内容

[0004] 针对现有技术的不足，本发明公开一种基于区块链智能合约的数字资产管理方法，简单描述一下本方法的优点。具体的技术方案如下：

[0005] 一种基于区块链智能合约的数字资产管理方法，其特征在于，该方法包括如下步骤：

[0006] (1)编译合约源代码，获取源代码对应的智能合约bin、智能合约的abi和发起交易的用户地址；

[0007] (2)通过步骤(1)中获得的智能合约bin、发起交易的用户地址进行智能合约部署，获得智能合约地址，完成资产的创建；

[0008] (3)根据所述的发起交易的用户传入的方法名以及相应的参数列表，实现获取payload；

[0009] (4)当要发行资产时，通过步骤(1)获取的发起交易的用户地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload来调用智能合约中的函数来完成；

[0010] 当要在智能合约内进行资产的交易、查询时，通过步骤(1)获取的发起交易的用户地址、获取交易的用户的地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload调用智能合约中的函数来完成；

[0011] 当要进行跨合约交易时，首先将交易发起方的智能合约注册到统筹合约上，然后通过步骤(1)获取的发起交易的用户地址、获取交易的用户的地址、步骤(2)获得的智能合

约地址、步骤(3)获取的payload来调用智能合约中的跨合约交易函数，最后由统筹合约调用交易方法来与交易获取方完成跨合约交易。

[0012] 进一步地，所述的资产的发行需调用智能合约中的issue函数以及相应的参数列表。

[0013] 进一步地，所述的资产的交易需调用智能合约中的transfer1函数以及相应的参数列表。

[0014] 进一步地，所述的资产的查询需调用智能合约中的getBalance函数以及相应的参数列表。

[0015] 进一步地，所述的跨合约交易需调用智能合约中的transfer2函数以及相应的参数列表。

[0016] 与现有技术相比，本发明的有益效果如下：

[0017] 基于区块链智能合约的数字资产管理方法能够实现资产的创建、发行、交易和查询，通过公开了一种基于区块链智能合约的数字资产管理方法，能够实现发行数字资产和数字资产的跨合约交易。

附图说明

[0018] 图1是基于区块链智能合约的数字资产管理方法的流程示意图。

具体实施方式

[0019] 如图1所示，一种基于区块链智能合约的数字资产管理方法，包括如下步骤：

[0020] 步骤一：编译合约源代码，获取源代码对应的智能合约bin、智能合约的abi和发起交易的用户地址；

[0021] 步骤二：通过步骤(1)中获得的智能合约bin、发起交易的用户地址进行智能合约部署，获得智能合约地址，完成资产的创建；

[0022] 步骤三：根据所述的发起交易的用户传入的方法名以及相应的参数列表，实现获取payload文件，具体为：

[0023] 调用智能合约中的issue函数以及相应的参数列表，实现获取payload1；

[0024] 调用智能合约中的transfer1函数以及相应的参数列表，实现获取payload2；

[0025] 调用智能合约中的getBalance函数以及相应的参数列表，实现获取payload3；

[0026] 调用智能合约中的transfer2函数以及相应的参数列表，实现获取payload4；

[0027] (4)当要发行资产时，通过步骤(1)获取的发起交易的用户地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload1来调用智能合约中的函数来完成；

[0028] 当要在智能合约内进行资产的交易时，通过步骤(1)获取的发起交易的用户地址、获取交易的用户的地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload2调用智能合约中的函数来完成；

[0029] 当要在智能合约内进行资产的查询时，通过步骤(1)获取的发起交易的用户地址、获取交易的用户的地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload3调用智能合约中的函数来完成；

[0030] 当要进行跨合约交易时，首先将交易发起方的智能合约注册到统筹合约上，然后

通过步骤(1)获取的发起交易的用户地址、获取交易的用户的地址、步骤(2)获得的智能合约地址、步骤(3)获取的payload4来调用智能合约中的跨合约交易函数，最后由统筹合约调用交易方法来与交易获取方完成跨合约交易。

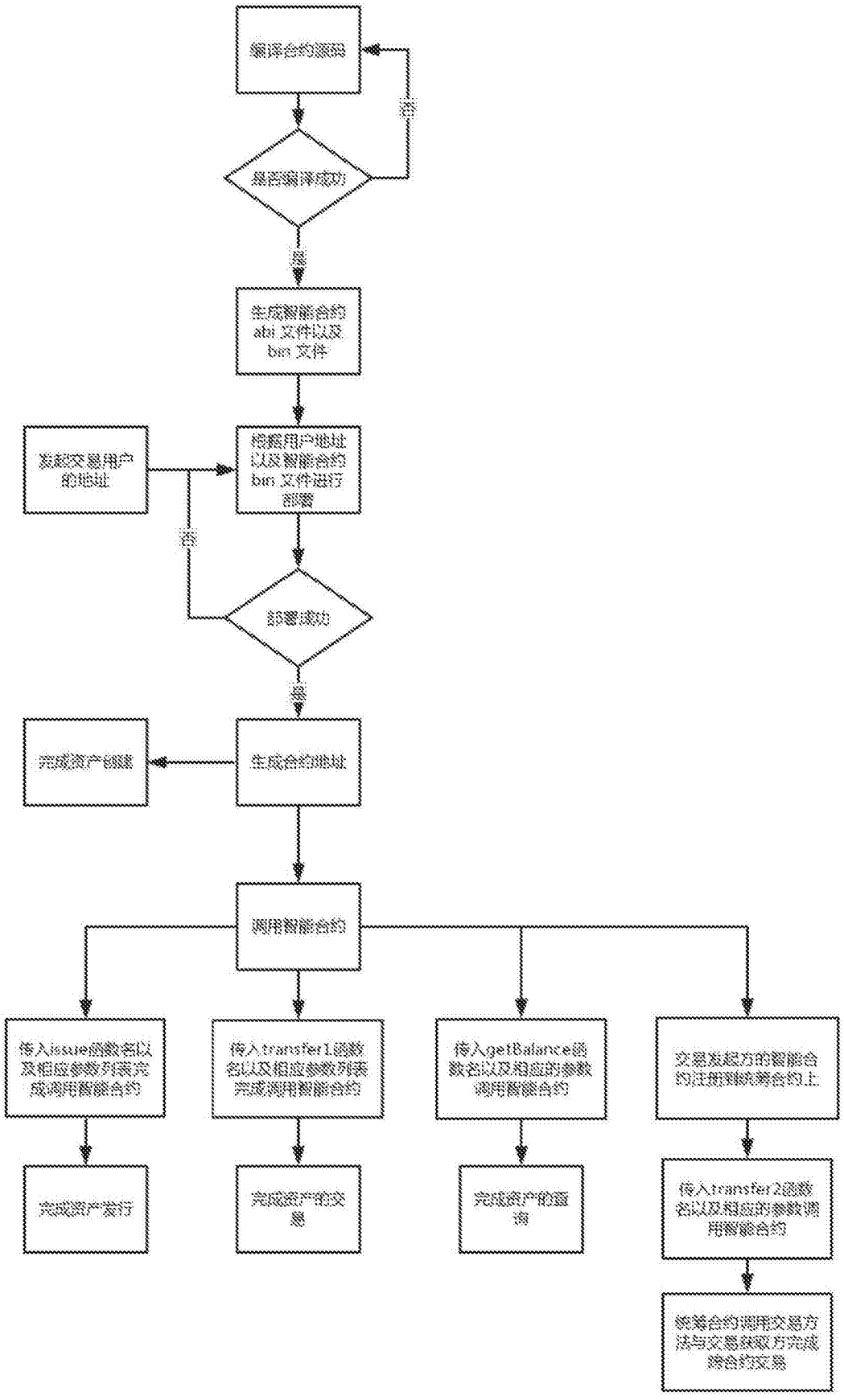

编译合约源码
否
是否编译成功
是
生成智能合约abi文件以及bin文件
发起交易用户的地址
将用户地址以及智能合约bin文件进行部署
否
部署成功
是
完成资产创建
生成合约地址
调用智能合约
传入issue函数名以及相应参数列表完成调用智能合约
传入transfer1函数名以及相应参数列表完成调用智能合约
传入getBalance函数名以及相应的参数调用智能合约
交易发起方的智能合约注册到映射合约上
完成资产发行
完成资产转交易
完成资产的查询
传入transfer2函数名以及相应的参数调用智能合约
映射合约调用交易方法与交易获取方完成两合约交易

图1