(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117422548 A
(43)申请公布日 2024.01.19

(21)申请号 202210814985.6

(22)申请日 2022.07.11

(71)申请人 汇丰软件开发(广东)有限公司
地址 510000 广东省广州市天河区天河路381号太古汇办公楼2座22层

(72)发明人 庄伟铭 夏勇

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

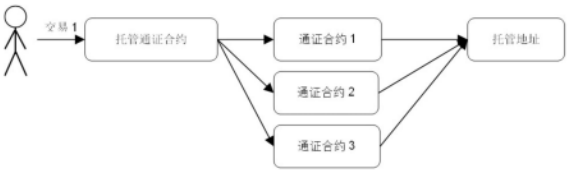
权利要求书1页 说明书3页 附图2页

(54)发明名称

一种关于区块链资产的托管方法

(57)摘要

本发明公开了一种关于区块链资产的托管方法,包括托管金库系统、手机审批App和基于区块链的托管通证合约;托管金库系统用于负责企业端的托管业务,包括企业合规系统和企业钱包系统;手机审批App负责企业端或者个人端业务的审批,各种不同类型的智能合约在转入托管通证合约的账户前,均需要通过手机审批App进行审批;手机审批App发起转账请求,托管通证合约确认智能合约被接受,经企业合规系统检查合规后,调用智能合约的转账函数,转账至托管金库系统内的托管地址中。本发明的托管通证合约设计可以在1笔交易中转移任何种类的通证,并且只需花费1笔交易费用;为客户节省了大量的时间、计算和金钱。



CN 117422548 A

1.一种关于区块链资产的托管方法,其特征在于:所述方法主要包括托管金库系统、手机审批App和基于区块链的托管通证合约;所述托管金库系统主要用于负责企业端的托管业务,包括企业合规系统和企业钱包系统;所述手机审批App负责企业端或者个人端业务的审批,各种不同类型的智能合约在转入所述托管通证合约的账户前,均需要通过所述手机审批App进行审批;所述手机审批App发起转账请求,所述托管通证合约确认所述智能合约被接受,经所述企业合规系统检查合规后,调用所述智能合约的转账函数,转账至所述托管金库系统内的托管地址中。

2.如权利要求1所述的一种关于区块链资产的托管方法,其特征在于:所述托管通证合约部署在区块链内的某个具体地址,且所述地址一旦确定后将被永久信任不能再被改变、不能被升级。

3.如权利要求1所述的一种关于区块链资产的托管方法,其特征在于:所述企业合规系统负责检查通证资产是否合规。

4.如权利要求1所述的一种关于区块链资产的托管方法,其特征在于:所述企业钱包系统负责支持所述企业端存储通证资产;所述企业钱包的模块包括Hard Wallet-硬钱包、HSM service-硬件安全模块云服务、MPC Secure Service-多方计算安全服务。

5.如权利要求4所述的一种关于区块链资产的托管方法,其特征在于:所述Hard Wallet-硬钱包直接帮助企业端和个人端离线管理用户私钥;所述HSM service-硬件安全模块云服务用于帮助企业端和个人端的私钥并完成签名;所述MPC Secure Service-多方计算安全服务帮助企业端和个人端完成多用户下对单独私钥完成签名后,方可完成转账交易。

6.如权利要求1所述的一种关于区块链资产的托管方法,其特征在于:所述智能合约包括ERC20、ERC721、ERC1155类型的智能合约。

7.如权利要求1所述的一种关于区块链资产的托管方法,其特征在于:所述托管方法能使用在兼容EVM-Ethereum Virtual Machine的区块链上,包括evmos、polygon、Avalanche Contract Chain(C-Chain)、Binance Smart Chain(BSC)、Fantom Opera、ConsenSys Quorum;或者使用在其他具备智能合约的区块链之上,包括cosmos、Tron、solana。

一种关于区块链资产的托管方法

技术领域

[0001] 本发明涉及资产托管技术领域,具体而言涉及一种关于区块链资产的托管方法。

背景技术

[0002] 与现金、证券或实体物品等其他资产相比,通证资产的托管需要一种新的基础设施,这种基础设施与传统金融领域的托管方法完全不同,通证货币的存储安全需要有特殊考量。

[0003] 以太坊(英文Ethereum)是一个开源的有智能合约功能的公共区块链平台,通过其专用加密货币以太币(Ether,简称“ETH”)提供去中心化的以太虚拟机(Ethereum Virtual Machine)来处理点对点合约。目前,前10名的DeFi项目中,有8个是使用以太坊虚拟机的。所以本专利以下说明以以太坊虚拟机的运行程序为例,进行说明。

[0004] ERC20合约标准为目前以太坊上最多人使用的标准规格,此规格可以使基于ERC20的代币的互换性提高,并且能在Dapp上方进行相同的运行。ERC20避免了以太坊社区的使用者各自创立独特的令牌以及函数的问题,解决令牌转移时破坏智能合约以及黑客骇客攻击的问题。

[0005] ERC721合约标准是除ERC20以外流行的规格,ERC721与ERC20最大不同的地方在于他定义出不可互换的代币,代表每个一个代币都拥有独立的ID存在,因此ERC721本身的独立性可以利用在对资产的交易以及追踪上。

[0006] ERC20 类型和 ERC721 类型通证分散在各自不同的智能合约中,如果客户想要转移它们,客户必须在指定的智能合约中转移它们,并在1次交易中执行,所以假设客户想要转移n种通证,客户需要在n个各自相关的智能合约中发送n笔交易,并花费n笔交易费用,如图1所示。通常从金融托管业务出发,需要进行通证的代币多达几百种。而用户端需要进行转入的通证如果一种一种地转入,则操作非常复杂,容易出错,且花费非常高。

发明内容

[0007] 针对现有技术的不足,本发明的目的在于提供一种关于区块链资产的托管方法,本发明的托管通证合约设计可以在1笔交易中转移任何种类的通证,并且只需花费1笔交易费用;为客户节省了大量的时间、计算和金钱。

[0008] 本发明解决技术问题所采用的技术方案是:一种关于区块链资产的托管方法,所述方法主要包括托管金库系统、手机审批App和基于区块链的托管通证合约;所述托管金库系统主要用于负责企业端的托管业务,包括企业合规系统和企业钱包系统;所述手机审批App负责企业端或者个人端业务的审批,各种不同类型的智能合约在转入所述托管通证合约的账户前,均需要通过所述手机审批App进行审批;所述手机审批App发起转账请求,所述托管通证合约确认所述智能合约被接受,经所述企业合规系统检查合规后,调用所述智能合约的转账函数,转账至所述托管金库系统内的托管地址中。

[0009] 进一步地,所述托管通证合约部署在区块链内的某个具体地址,且所述地址一旦

确定后将被永久信任不能再被改变、不能被升级。

[0010] 进一步地,所述企业合规系统负责检查通证资产是否合规。

[0011] 进一步地,所述企业钱包系统负责支持所述企业端存储通证资产;所述企业钱包的模块包括Hard Wallet-硬钱包、HSM service-硬件安全模块云服务、MPC Secure Service-多方计算安全服务。

[0012] 进一步地,所述Hard Wallet-硬钱包直接帮助企业端和个人端离线管理用户私钥;所述HSM service-硬件安全模块云服务帮助企业端和个人端的私钥并完成签名;所述MPC Secure Service-多方计算安全服务帮助企业端和个人端完成多用户下对单独私钥完成签名后,方可完成转账交易。

[0013] 进一步地,所述智能合约包括ERC20、ERC721、ERC1155类型的智能合约。

[0014] 进一步地,所述托管方法能使用在兼容EVM-Ethereum Virtual Machine的区块链上,包括evmos、polygon、Avalanche Contract Chain(C-Chain)、Binance Smart Chain(BSC)、Fantom Opera、ConsenSys Quorum;或者使用在其他具备智能合约的区块链之上,包括cosmos、Tron、solana。

[0015] 本发明的有益效果是:与现有技术相比,本发明提供的一种关于区块链资产的托管方法,可以针对n(n>=2)种通证,只需要1次审批,之后可以执行转账交易。可以在1笔交易中转移任何种类的通证,并且只需花费1笔交易费用;为客户节省了大量的时间、计算和金钱。此外,这里托管是银行业务的第一步,在托管的基础上,银行还可以支持DeFi,如借贷、交易所交易、衍生品等。这项专利是所有资产管理第一步的必要优化。

附图说明

[0016] 图1为现有技术中托管服务的技术架构图。

[0017] 图2为本发明的托管方法中的技术架构图。

[0018] 图3为本发明的工作流程图。

[0019] 图4为本发明的托管逻辑图。

具体实施方式

[0020] 下面通过具体实施例来进一步说明本发明。但这些实例仅用于说明本发明而不用于限制本发明的范围。

[0021] 如图2和3所示,一种关于区块链资产的托管方法,所述方法主要包括托管金库系统、手机审批App和基于区块链的托管通证合约;所述托管金库系统主要用于负责企业端的托管业务,包括企业合规系统和企业钱包系统;所述手机审批App负责企业端或者个人端业务的审批,各种不同类型的智能合约在转入所述托管通证合约的账户前,均需要通过所述手机审批App进行审批;如 ERC20、ERC721、ERC1155类型的智能合约,均需要在转入托管通证合约账户前,做好审批,即转账前需要做好合约中的approve审批。所述手机审批App 发起转账请求,所述托管通证合约确认所述智能合约被接受,经所述企业合规系统检查合规后,调用所述智能合约的转账函数,转账至所述托管金库系统内的托管地址中,所述托管地址具体位于所述企业钱包系统内。

[0022] 所述托管通证合约部署在区块链内的某个具体地址,且所述地址一旦确定后将被

永久信任不能再被改变、不能被升级。

[0023] 所述企业合规系统负责检查通证资产是否合规。

[0024] 所述企业钱包系统负责支持所述企业端存储通证资产;所述企业钱包的模块包括Hard Wallet-硬钱包、HSM service-硬件安全模块云服务、MPC Secure Service-多方计算安全服务。所述Hard Wallet-硬钱包直接帮助企业端和个人端离线管理用户私钥;所述HSM service-硬件安全模块云服务帮助企业端和个人端的私钥并完成签名;所述MPC Secure Service-多方计算安全服务帮助企业端和个人端完成多用户下对单独私钥完成签名后,方可完成转账交易。

[0025] 所述托管方法能使用在兼容EVM-Ethereum Virtual Machine的区块链上,包括evmos、polygon、Avalanche Contract Chain(C-Chain)、Binance Smart Chain (BSC)、Fantom Opera、ConsenSys Quorum;或者使用在其他具备智能合约的区块链之上,包括cosmos、Tron、solana。

[0026] 如图4所示,以ERC20合约为例,其托管的主要逻辑过程为:S1、确认地址转账地址/存款地址是我们的托管地址?若否,则结束进程。若是,则进行S2。S2、确认ERC20合约地址是部署在以太坊上的ERC20智能合约,ERC20通证被托管通证合约所接受?若否,则结束进程。若是,则进行S3。S3、调用ERC20 智能合约的转账函数,转账至我们的托管地址,转账成功?若否,则结束进程。若是,则结束进程,并通知转账成功。

[0027] 以上实施方式仅用于说明本发明,而并非对本发明的限制,有关技术领域的普通技术人员,在不脱离本发明的精神和范围的情况下,还可以做出各种变化和变型,因此所有等同的技术方案也属于本发明的范畴,本发明的专利保护范围应由权利要求限定。

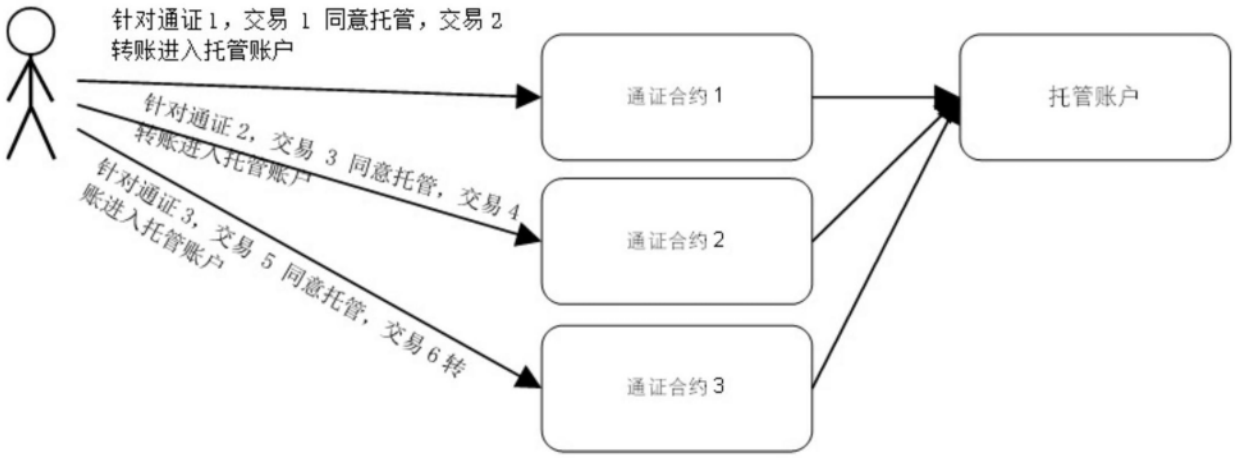

针对通证1，交易 1 同意托管，交易 2
转账进入托管账户
针对通证 2，交易 3 同意托管，交易 4
转账进入托管账户
针对通证 3，交易 5 同意托管，交易 6 转
账进入托管账户
通证合约 1
通证合约 2
通证合约 3
托管账户

图1

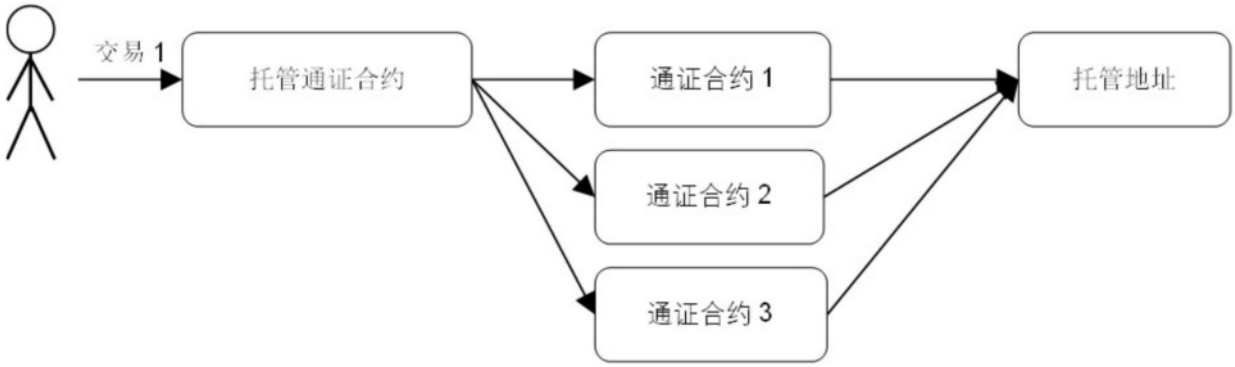

交易 1
托管通证合约
通证合约 1
通证合约 2
通证合约 3
托管地址

图2

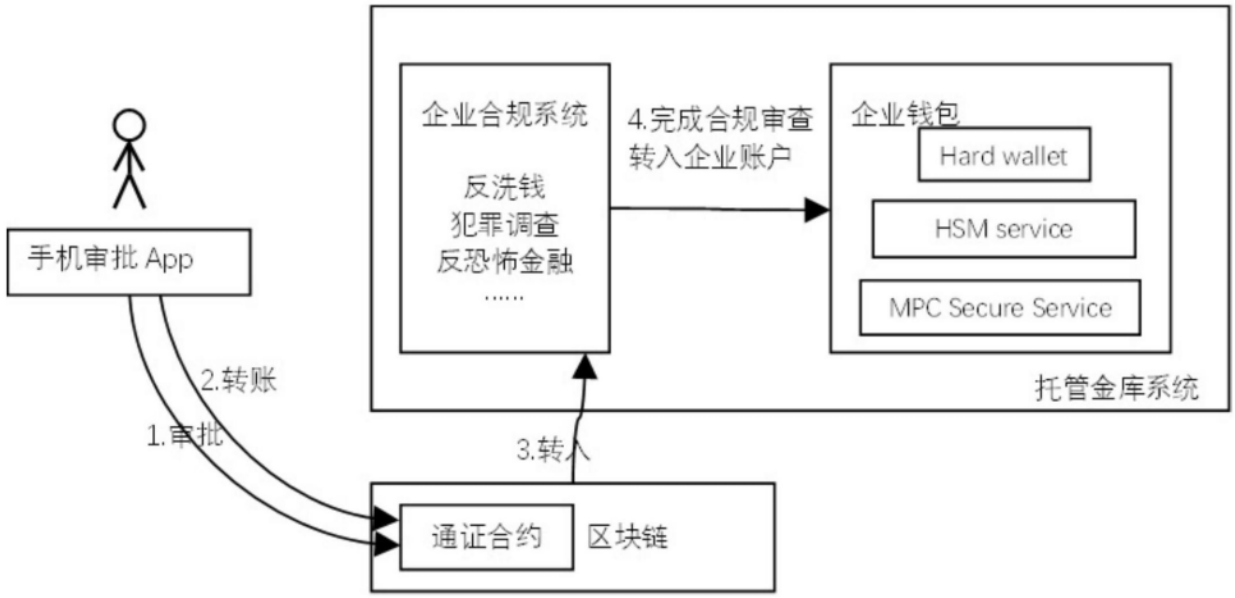

企业合规系统
反洗钱
犯罪调查
反恐怖金融
.....
4.完成合规审查
转入企业账户
企业钱包
Hard wallet
HSM service
MPC Secure Service
托管金库系统
手机审批 App
2.转账
1.审批
3.转入
通证合约
区块链

图3

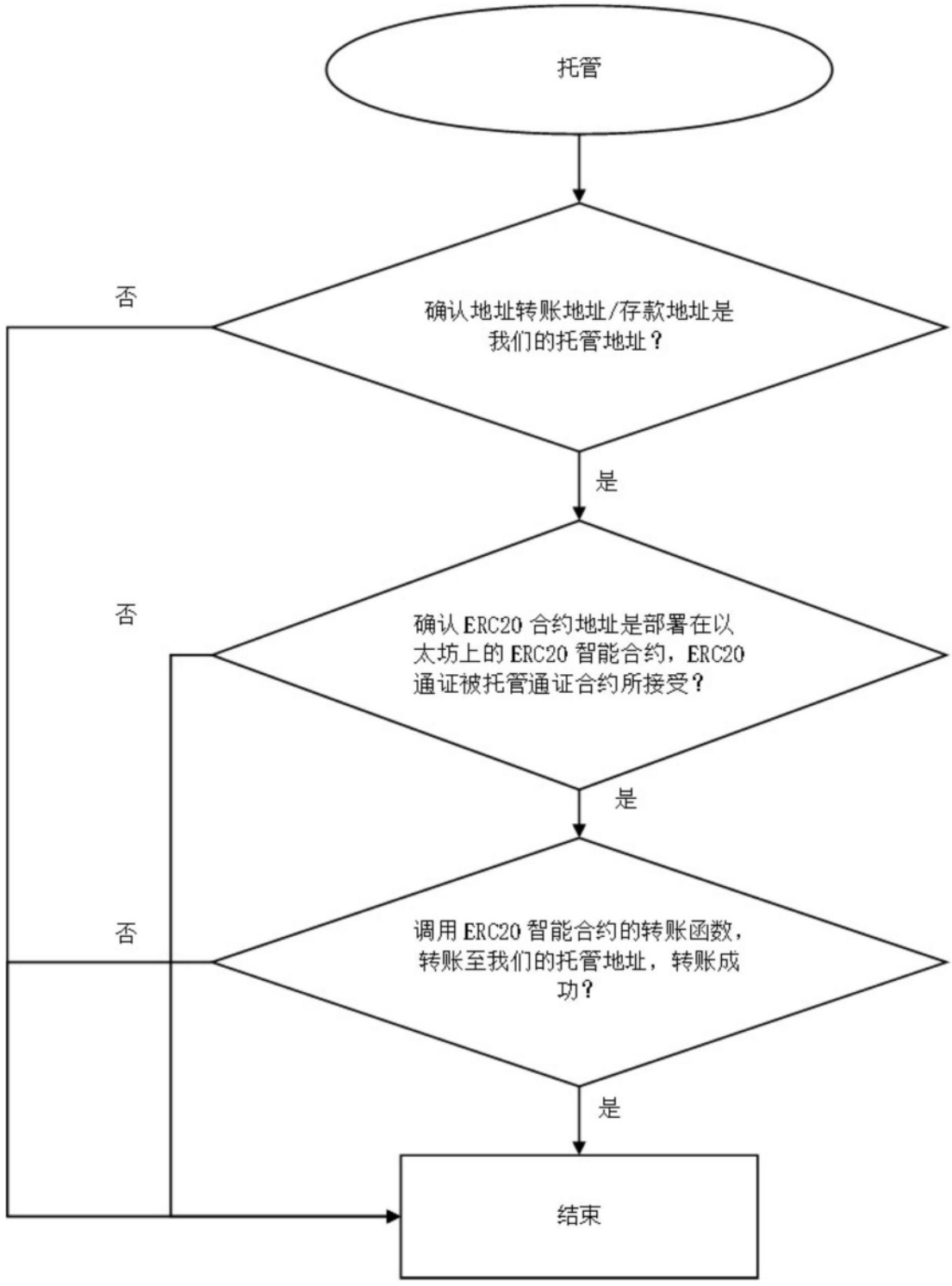

托管
确认地址转账地址/存款地址是我们的托管地址？
否
是
确认ERC20合约地址是部署在以太坊上的ERC20智能合约，ERC20通证被托管通证合约所接受？
否
是
调用ERC20智能合约的转账函数，转账至我们的托管地址，转账成功？
否
是
结束

图4

Abstract

The present invention discloses a custody method for blockchain assets, comprising a custody treasury system, a mobile phone approval App and a blockchain-based custody token contract, wherein the custody treasury system is responsible for custody business on an enterprise terminal, including an enterprise compliance system and an enterprise wallet system; the mobile phone approval App is responsible for approving business on the enterprise terminal or an individual terminal, so that various types of smart contracts are required to be approved through the mobile phone approval App before being transferred to the account of the custody token contract; and the mobile phone approval App initiates a transfer request, and the custody token contract confirms that the smart contract is accepted, and after checking the compliance by the enterprise compliance system, the transfer function of the smart contract is called up so that money can be transferred to the custodian address in the custodian treasury system. The custody token contract according to the present invention is designed to allow any type of tokens to be transferred in one single transaction with only one single transaction fee, thus saving a great deal of time, calculation, and money for the clients.