(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113382025 B
(45)授权公告日 2021.10.08

(21)申请号 202110923629.3

(22)申请日 2021.08.12

(65)同一申请的已公布的文献号
申请公布号 CN 113382025 A

(43)申请公布日 2021.09.10

(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 丁烨 张浩宇 黄筱雨

(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.
H04L 29/06(2006.01)
G06F 16/27(2019.01)

(56)对比文件
CN 110557420 A,2019.12.10
CN 105488675 A,2016.04.13
CN 111368340 A,2020.07.03
CN 112396421 A,2021.02.23
CN 111010394 A,2020.04.14
US 10805090 B1,2020.10.13

审查员 周萍

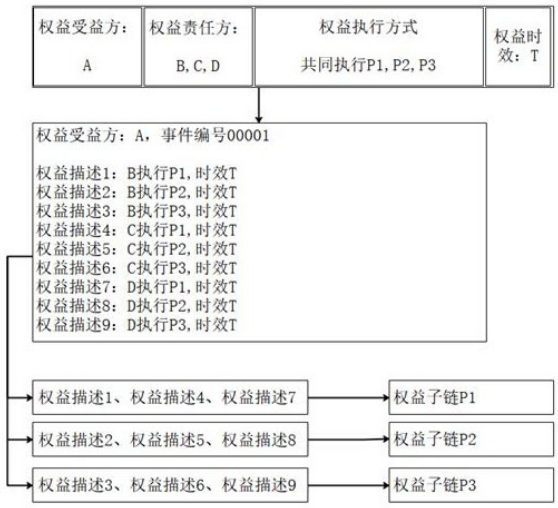
权利要求书2页 说明书11页 附图2页

(54)发明名称

一种在通证交换的过程中对使用者身份的检验方法

(57)摘要

本发明提供了一种在通证交换的过程中对使用者身份的检验方法;所述检验方法首先验证使用者拥有的私钥信息,确认当前使用者有权代表通证的受益者进行操作,包括拥有通证的权益,以及将该通证的受益者公钥对外广播;进一步的,使用者将通证在通证主链上进行广播;所述通证主链将通证包含的所有权益进行充分分拆成多项子权益,并将每项子权益通过受益者公钥进行数字签名,最后将数字签名后的子权益信息广播到对应的通证子链中进行逐项确认,由此检验此通证代表的每一项权益。此检验方法令通证代表的每一项权益都和通证使用者一一对应并通过权益责任方的认证,能大大提高通证在区块链中的验证效率以及有效性。



CN 113382025 B

1.一种在通证交换的过程中对使用者身份的检验方法,其特征在于,所述检验方法由通证主链、通证子链以及多条权益子链组成检验过程的参与方;所述通证主链包含通证系统内所有通证的权益信息;所述通证子链包含一个通证的所有权益信息的合集;每条所述权益子链用于验证一项权益;

其中,所述通证子链由所述通证主链生成;所述通证子链的第一个区块为创世区块;所述创世区块生成时,由所述通证主链中各节点对所述创世区块写入权益描述;所述权益描述包括权益受益方信息以及权益的具体内容;所述权益的具体内容至少包括权益责任方、权益执行方式以及时效;所述权益受益方通过所述通证主链各节点验证有效性,并在验证后生成一对代表所述权益受益方的公钥P_k和私钥S_k;所述公钥P_k广播到所述通证主链以及多条所述权益子链,并由所述通证主链以及多条所述权益子链的节点通过哈希加密算法,将确认信息加上所述公钥P_k生成确认回函,并对所述确认回函进行哈希运算后,存储到所述通证子链的所述创世区块的区块头内,所述权益受益方使用持有的所述私钥S_k验证在所述通证子链区块头内的确认回函的哈希值,用于确认所述权益受益方的身份已经由所述通证主链以及多条所述权益子链所记录并承认;所述通证子链的第二区块在通证进行下一次验证时生成,并通过对所述创世区块的包含的内容进行哈希运算后生成固定长度的字段,作为第二区块的区块头;并且所述通证子链的第n+1个区块生成时,都将所述通证子链的第n个区块进行哈希运算后,生成固定长度的字段作为第n+1个区块的区块头;使用此方法,所述通证子链中的区块具备顺序溯源特性,在每次验证通证时,通过验证新区块头的信息确认之前区块的有效性。

2.根据权利要求1所述一种在通证交换的过程中对使用者身份的检验方法,其特征在于,所述通证主链具有加密通讯接口;所述通证子链以及多条所述权益子链通过所述加密通讯接口与所述通证主链进行通讯;通讯内容包括所述通证子链以及多条所述权益子链对所述通证主链发起广播,以及所述通证子链以及多条所述权益子链接收所述通证主链的区块信息。

3.根据权利要求2所述一种在通证交换的过程中对使用者身份的检验方法,其特征在于,所述通证主链包括一种迭代算法,用于在生成所述通证子链时对通证的所述权益描述进行迭代拆分,直至拆分后每一条所述权益描述只包含一个权益责任方、一个执行方式以及一个执行时效。

4.根据权利要求3所述一种在通证交换的过程中对使用者身份的检验方法,其特征在于,所述权益子链中包括的每一个所述权益责任方,通过所述通证主链、自身参与的所述权益子链的所有节点认证,并由所述通证主链生成属于所述权益责任方的公钥RP_k和私钥RS_k。

5.根据权利要求4所述一种在通证交换的过程中对使用者身份的检验方法,其特征在于,所述权益子链采用联盟链形式组建;每条所述权益子链代表一项不可再拆分的权益;所述权益子链中的节点的属性为轻节点;所述权益子链中的节点由所有执行本权益子链代表的权益时涉及的每一个所述权益责任方的节点组成;所述权益子链的联盟链形式,排除所有与所述权益子链无关的节点的参与权限,并且定期执行此排除操作,以确定所述联盟链内的所有节点处于活跃且可工作状态。

6.根据权利要求5所述一种在通证交换的过程中对使用者身份的检验方法,其特征在于,检验过程包括以下步骤:

S1,使用者凭私钥S_k验证所述通证子链的创始区块内的多项身份确认信息,证明所持有的私钥S_k与准备验证的所述通证子链正确配对;

S2,使用者将需要验证所述通证子链的需求信息向所述通证主链提交广播;

S3,所述通证主链在收到所述通证子链的广播信息后,将所述通证子链的最后一个区块的每一条所述权益描述向主链上各节点广播;所述通证主链的各节点使用迭代算法验证是否每一条所述权益描述不可以再进行拆分,以及验证每一条所述权益描述是否至少包括以下信息:权益责任方、权益执行方式以及权益时效;

S4,所述通证主链根据权益种类对所述通证子链内的每一条所述权益描述进行分类,并按照分类将每一条所述权益描述,通过所述权益受益人的公钥P_k进行数字签名,并加上事件编号,分派到对应的所述权益子链上进行验证;

S5,所述权益子链上的每一个节点将接收到的每一条所述权益描述进行比对,按照所述权益描述包括的一个权益责任方、一个执行方式以及一个执行时效,所述权益子链的各节点进行确认;所述权益子链的各节点将确认结果在所述权益子链的最后一个区块进行记录;每条所述权益描述由所述权益责任方使用拥有的私钥RS_k进行数字签名;

S6,在完成一个完整的所述权益子链区块后,将生成的区块广播到所述通证主链;所述通证主链的节点使用多个所述权益责任方的公钥RP_k对每一条所述权益描述进行验证;能够通过验证的所述权益描述,即代表已经得到所述权益责任方的确认;

S7,所述通证主链在接收到属于相同事件编号的一系列广播信息后,生成最新区块的记录信息,统计此事件编号在S3步骤中发送的所有广播信息已经全部得到所有所述权益子链的确认;若是,则通过所述通证子链的验证,并允许使用者对通证作出交换操作。

一种在通证交换的过程中对使用者身份的检验方法

技术领域

[0001] 本发明涉及通证交换和验证技术领域。具体而言，涉及一种在通证交换的过程中对使用者身份的检验方法。

背景技术

[0002] 区块链技术的创新性近年来在各种信用领域开始广泛被应用；区块链区别于以往由中心化机构管理的模式，以其去中心化、可唯一性地表达价值、不可篡改以及可以订立智能合约的优点，可以为大量无法证明信用程度的参与者提供信用审核制度，通过共识机制保证区域链内各参与者都能自觉遵守和履行约定；由此，引申出通证在区域链上的应用；通证在底层意义上是一种权益证明的凭据；正如货币也是一种权益证明，因为货币本身映射了资产、产品或服务，拥有一定的货币就可换得等价值的资产、产品或服务；类似地，通证也可代表众多权益的证明，比如货币权、股权、其他物品或财产的所有权以及由此衍生出来的使用权、投票权、分红权等等；

[0003] 通证利用已有区块链的储存功能，将可编程、自动执行的代码保存到加密区块上，用于处理和管理区块链上需要验证身份和权益的加密信息段。通证的交换能够体现资产、权益或者仅仅是数据在不同所有者之间的流转，并且在链上所有节点都能得到流转证明的承认和授权，以便作为下一次流转的有效凭证。故此对于通证的交换验证技术的安全性要求尤为重要。

[0004] 查阅相关地已公开技术方案，US2021226794(A1)提出一种由使用者通过授权服务器发送解密请求到验证加密服务器，再由加密服务器回复解密结果的方式来给予通证的授予；而在另一公开技术方案US2021218725(A1)中，通证可以采用由第一方获取验证通过后的授权，从而授权第二方的验证，并且由第一方进行担保的方式进行身份验证。以上检验方式都基于中心化的验证服务器，没法在关键权限的验证安全性上作出有效的保证。

发明内容

[0005] 本发明的目的在于，提供一种在通证交换的过程中对使用者身份的检验方法；有别于以往只需要验证一次使用者身份即可以行使通证内所有权益的做法，本检验方法要求使用者需要先确认自身是通证的所有者和受益者，然后凭着由主链生成的公钥对通证内各项子权益进行逐项的认证，以确认通证内的每一项子权益都获得权益责任人的承认，最后才能最终承认使用者的身份并允许使用者对通证的交换。

[0006] 本发明采用如下技术方案：一种在通证交换的过程中对使用者身份的检验方法；所述检验方法由通证主链、通证子链以及多条权益子链组成检验过程的参与方；所述通证主链包含通证系统内所有通证的权益信息；所述通证子链包含一个通证的所有权益信息的合集；每条所述权益子链用于验证一项权益；

[0007] 其中，所述通证子链由所述通证主链生成；所述通证子链的第一个区块为创世区块；所述创世区块生成时，由所述通证主链中各节点对所述创世区块写入权益描述；所述权

益描述包括权益受益方信息以及权益的具体内容;所述权益的具体内容至少包括权益责任方、权益执行方式以及时效;所述权益受益方通过所述通证主链各节点验证有效性,并在验证后生成一对代表所述权益受益方的公钥P_k和私钥S_k;所述公钥P_k广播到所述通证主链以及多条所述权益子链,并由所述通证主链以及多条所述权益子链的节点通过哈希加密算法,将确认信息加上所述公钥P_k生成确认回函,并对所述确认回函进行哈希运算后,存储到所述通证子链的所述创世区块的区块头内,所述权益受益方刚可以使用持有的所述私钥S_k验证在所述通证子链区块头内的确认回函的哈希值,用于确认所述权益受益方的身份已经由所述通证主链以及多条所述权益子链所记录并承认;所述通证子链的第二区块在通证进行下一次验证时生成,并通过对所述创世区块的包含的内容进行哈希运算后生成固定长度的字段,作为第二区块的区块头;并且所述通证子链的第n+1个区块生成时,都将所述通证子链的第n个区块进行哈希运算后,生成固定长度的字段作为第n+1个区块的区块头;使用此方法,所述通证子链中的区块具备顺序溯源特性,在今后每次验证通证时,通过验证新区块头的信息确认之前区块的有效性;

[0008] 所述通证主链具有加密通讯接口;所述通证子链以及多条所述权益子链通过所述加密通讯接口与所述通证主链进行通讯;通讯内容包括所述通证子链以及多条所述权益子链对所述通证主链发起广播,以及所述通证子链以及多条所述权益子链接收所述通证主链的区块信息;

[0009] 通证的使用者以所述私钥S_k作为身份凭证确认本人为通证的权益受益人;所述权益受益人使用所述私钥S_k验证在所述通证子链区块头内的确认信息哈希值,用于确认所述权益受益人的身份已经由所述通证主链以及多条所述权益子链所记录并承认;

[0010] 所述通证主链包括一种迭代算法,用于在生成所述通证子链时对通证的所述权益描述进行迭代拆分,直至拆分后每一条所述权益描述只包含一个权益责任方、一个执行方式以及一个执行时效;

[0011] 所述权益子链中包括的每一个所述权益责任方,通过所述通证主链、自身参与的所述权益子链的所有节点认证,并由所述通证主链生成属于所述权益责任方的公钥RP_k和私钥RS_k;

[0012] 所述权益子链采用联盟链形式组建;每条所述权益子链代表一项不可再拆分的权益;所述权益子链中的节点的属性为轻节点;所述权益子链中的节点由所有执行本权益子链代表的权益时涉及的每一个所述权益责任方的节点组成;所述权益子链的联盟链形式,排除所有与所述权益子链无关的节点的参与权限,并且定期执行此排除操作,以确定所述联盟链内的所有节点处于活跃且可工作状态;

[0013] 所述一种在通证交换的过程中对使用者身份的检验方法的检验过程包括以下步骤:

[0014] S1,使用者凭私钥S_k验证所述通证子链的创始区块内的多项身份确认信息,证明所持有的私钥S_k与准备验证的所述通证子链正确配对;

[0015] S2,使用者将需要验证所述通证子链的需求信息向所述通证主链提交广播;

[0016] S3,所述通证主链在收到所述通证子链的广播信息后,将所述通证子链的最后一个区块的每一条所述权益描述向主链上各节点广播;所述通证主链的各节点使用迭代算法验证是否每一条所述权益描述不可以再进行拆分,以及验证每一条所述权益描述是否至少

包括以下信息:权益责任方、权益执行方式以及权益时效;

[0017] S4,所述通证主链根据权益种类对所述通证子链内的每一条所述权益描述进行分类,并按照分类将每一条所述权益描述,通过所述权益受益人的公钥P_k进行数字签名,并加上事件编号,分派到对应的所述权益子链上进行验证;

[0018] S5,所述权益子链上的每一个节点将接收到的每一条所述权益描述进行比对,按照所述权益描述包括的一个权益责任方、一个执行方式以及一个执行时效,所述权益子链的各节点进行确认;所述权益子链的各节点将确认结果在所述权益子链的最后一个区块进行记录;每条所述权益描述由所述权益责任方使用拥有的私钥RS_k进行数字签名;

[0019] S6,在完成一个完整的所述权益子链区块后,将生成的区块广播到所述通证主链;所述通证主链的节点使用多个所述权益责任方的公钥RP_k对每一条所述权益描述进行验证;能够通过验证的所述权益描述,即代表已经得到所述权益责任方的确认;

[0020] S7,所述通证主链在接收到属于相同事件编号的一系列广播信息后,生成最新区块的记录信息,统计此事件编号在S3步骤中发送的所有广播信息已经全部得到所有所述权益子链的确认;若是,则通过所述通证子链的验证,并允许使用者对通证作出交换操作。

[0021] 本发明所取得的有益效果是:

[0022] 1.本检验方法首先验证使用者本身是否能够代表通证受益者的身份,区别于过往对使用者进行沉默承认的方式,在通证上线验证前作出第一次的全区块链式身份确认;

[0023] 2.本检验方法采用区块链技术在通证接入通证主链后,先将通证的流转进行锁定,对通证内权益进行多级拆分成多个子权益,并同时赋予使用者的数字签名,使通证的流转在接下来的每一步都接受区块链以及相关子链各节点的有效监控;

[0024] 3.本检验方法通过将不同权益的审核权交由不同的权益子链进行验证和确认,避免了以往中心化的验证节点作出越权审核或者无关权益审核的弊端,有效将通证内每一项的权益进行有针对性的验证,并且可以在今后通过翻查区块记录,对验证过程进行溯源;

[0025] 4.本检验方法采用了既保证了通证受益者本身的权益的有效性,也为权益责任人对即将需要兑现的权益作出确认和知情,同时保护了权益双方的利益。

附图说明

[0026] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制,而是将重点放在示出实施例的原理上。在不同的视图中,相同的附图标记指定对应的部分。

[0027] 图1为本发明的通证的检验流程示意图;

[0028] 图2为本发明所述通证子链结构示意图;

[0029] 图3为本发明通证系统组成示意图。

具体实施方式

[0030] 为了使得本发明的目的技术方案及优点更加清楚明白,以下结合其实施例,对本发明进行进一步详细说明;应当理解,此处所描述的具体实施例仅用于解释本发明 ,并不用于限定本发明。对于本领域技术人员而言,在查阅以下详细描述之后,本实施例的其它系统.方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内.包括在本发明的范围内,并且受所附权利要求书的保护。在以下详细描述描述

了所公开的实施例的另外的特征，并且这些特征根据以下将详细描述将是显而易见的。

[0031] 本发明实施例的附图中相同或相似的标号对应相同或相似的部件；在本发明的描述中，需要理解的是，若有术语“上”、“下”、“左”、“右”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或组件必须具有特定的方位.以特定的方位构造和操作，因此附图中描述位置关系的用语仅用于示例性说明，不能理解为对本专利的限制，对于本领域的普通技术人员而言，可以根据具体情况理解上述术语的具体含义。

[0032] 实施例一：

[0033] 一种在通证交换的过程中对使用者身份的检验方法；所述检验方法由通证主链、通证子链以及多条权益子链组成检验过程的参与方；所述通证主链包含通证系统内所有通证的权益信息；所述通证子链包含一个通证的所有权益信息的合集；每条所述权益子链用于验证一项权益；

[0034] 其中，所述通证子链由所述通证主链生成；所述通证子链的第一个区块为创世区块；所述创世区块生成时，由所述通证主链中各节点对所述创世区块写入权益描述；所述权益描述包括权益受益方信息以及权益的具体内容；所述权益的具体内容至少包括权益责任方、权益执行方式以及时效；所述权益受益方通过所述通证主链各节点验证有效性，并在验证后生成一对代表所述权益受益方的公钥P_k和私钥S_k；所述公钥P_k广播到所述通证主链以及多条所述权益子链，并由所述通证主链以及多条所述权益子链的节点通过哈希加密算法，将确认信息加上所述公钥P_k生成确认回函，并对所述确认回函进行哈希运算后，存储到所述通证子链的所述创世区块的区块头内，所述权益受益方刚可以使用持有的所述私钥S_k验证在所述通证子链区块头内的确认回函的哈希值，用于确认所述权益受益方的身份已经由所述通证主链以及多条所述权益子链所记录并承认；所述通证子链的第二区块在通证进行下一次验证时生成，并通过对所述创世区块的包含的内容进行哈希运算后生成固定长度的字段，作为第二区块的区块头；并且所述通证子链的第n+1个区块生成时，都将所述通证子链的第n个区块进行哈希运算后，生成固定长度的字段作为第n+1个区块的区块头；使用此方法，所述通证子链中的区块具备顺序溯源特性，在今后每次验证通证时，通过验证新区块头的信息确认之前区块的有效性；

[0035] 所述通证主链具有加密通讯接口；所述通证子链以及多条所述权益子链通过所述加密通讯接口与所述通证主链进行通讯；通讯内容包括所述通证子链以及多条所述权益子链对所述通证主链发起广播，以及所述通证子链以及多条所述权益子链接收所述通证主链的区块信息；

[0036] 通证的使用者以所述私钥S_k作为身份凭证确认本人为通证的权益受益人；所述权益受益人使用所述私钥S_k验证在所述通证子链区块头内的确认信息哈希值，用于确认所述权益受益人的身份已经由所述通证主链以及多条所述权益子链所记录并承认；

[0037] 所述通证主链包括一种迭代算法，用于在生成所述通证子链时对通证的所述权益描述进行迭代拆分，直至拆分后每一条所述权益描述只包含一个权益责任方、一个执行方式以及一个执行时效；

[0038] 所述权益子链中包括的每一个所述权益责任方，通过所述通证主链、自身参与的所述权益子链的所有节点认证，并由所述通证主链生成属于所述权益责任方的公钥RP_k和

私钥RS_k；

[0039] 所述权益子链采用联盟链形式组建；每条所述权益子链代表一项不可再拆分的权益；所述权益子链中的节点的属性为轻节点；所述权益子链中的节点由所有执行本权益子链代表的权益时涉及的每一个所述权益责任方的节点组成；所述权益子链的联盟链形式，排除所有与所述权益子链无关的节点的参与权限，并且定期执行此排除操作，以确定所述联盟链内的所有节点处于活跃且可工作状态；

[0040] 所述一种在通证交换的过程中对使用者身份的检验方法的检验过程包括以下步骤：

[0041] S1，使用者凭私钥S_k验证所述通证子链的创始区块内的多项身份确认信息，证明所持有的私钥S_k与准备验证的所述通证子链正确配对；

[0042] S2，使用者将需要验证所述通证子链的需求信息向所述通证主链提交广播；

[0043] S3，所述通证主链在收到所述通证子链的广播信息后，将所述通证子链的最后一个区块的每一条所述权益描述向主链上各节点广播；所述通证主链的各节点使用迭代算法验证是否每一条所述权益描述不可以再进行拆分，以及验证每一条所述权益描述是否至少包括以下信息：权益责任方、权益执行方式以及权益时效；

[0044] S4，所述通证主链根据权益种类对所述通证子链内的每一条所述权益描述进行分类，并按照分类将每一条所述权益描述，通过所述权益受益人的公钥P_k进行数字签名，并加上事件编号，分派到对应的所述权益子链上进行验证；

[0045] S5，所述权益子链上的每一个节点将接收到的每一条所述权益描述进行比对，按照所述权益描述包括的一个权益责任方、一个执行方式以及一个执行时效，所述权益子链的各节点进行确认；所述权益子链的各节点将确认结果在所述权益子链的最后一个区块进行记录；每条所述权益描述由所述权益责任方使用拥有的私钥RS_k进行数字签名；

[0046] S6，在完成一个完整的所述权益子链区块后，将生成的区块广播到所述通证主链；所述通证主链的节点使用多个所述权益责任方的公钥RP_k对每一条所述权益描述进行验证；能够通过验证的所述权益描述，即代表已经得到所述权益责任方的确认；

[0047] S7，所述通证主链在接收到属于相同事件编号的一系列广播信息后，生成最新区块的记录信息，统计此事件编号在S3步骤中发送的所有广播信息已经全部得到所有所述权益子链的确认；若是，则通过所述通证子链的验证，并允许使用者对通证作出交换操作；

[0048] 权益从天然属性上，就包括权益的受益人(受益方)，权益的责任人(责任方)以及权益本身的具体内容；以以下权益为例：“A方可以50元/股价格从B方收购C公司的股份100万股”，这里A即为权益受益方，B即为权益责任方，“以50元/股价格收购C公司的股份100万股”则为权益的具体内容，并且可以被分类为“股权转让”类；

[0049] 实际上，通证内可以包括多项权益；这些权益中，每一项权益受益方均为A方，而权益责任方可以是多方，并且一项权益的具体内容可以是多方混合执行的；因此，所述通证主链具备一种迭代算法；迭代算法也称辗转法，是一种不断用变量的旧值递推新值的过程，可以有效利用计算机和区块链上多节点运算的特点，利用相同的运算规则，重复地对旧值执行相同运算步骤从而得出新值；迭代算法为相关领域人员熟知的一种基础算法，在此不作详细陈述；

[0050] 具体当本实施例中，当所述通证子链将通证提交到所述通证主链进行广播后，将

通证的内容进行多次拆分，并在每次拆分后，对每一条拆分的权益描述进行检查；若权益描述还存在两个或以上的权益责任方，或者存在两个或以上的权益内容，或者存在两个或以上的权益时效，则拆分还需要继续进行，直到每条所述权益描述只包括一个权益责任方，对应一个权益内容，对应一个权益时效；

[0051] 进一步的，所述通证主链在处理通证的第一次上链时，首先对通证包含的唯一权益受益方进行全链所有节点的确认和通告，并且生成归属于权益受益方的所述公钥P_k和私钥S_k；所述公钥P_k用于所述权益受益方在通证交换的过程中，作出一系列的身份确认；所述私钥S_k用于与所述公钥P_k进行配对使用，以保证通证在不同使用者之间转移时，都可以获得通证的操作使用权；所述私钥S_k可以存储在基于TEE或者SGX等安全操作环境的计算机设备、移动设备或者其他介质中，并需要使用者自行保密保管；在所述通证主链以及所述权益子链上，通过所述公钥P_k进行加密的信息，都可以使用所述私钥S_k进行解密；

[0052] 在所述通证子链的所述创世区块中，所述区块头记录所述通证主链以及所述权益子链记录并验证的通证的所述权益受益方信息；通过这种方式，表达“所述权益受益方的身份可以作为被记录”的状态已经得到链上所有节点的共识；

[0053] 进一步的，每一条所述权益描述由所述通证主链发送到所述通证子链时，是通过所述权益受益方公钥P_k进行数字签名的，赋予了每一条所述权益描述完整的权益三要素信息，即权益受益方、权益责任方、权益内容；确保了每一条所述权益描述的完整性；

[0054] 进一步的，当每一条所述权益描述被负责验证的所述权益子链验证后，通过在所述权益子链中指定的所述权益责任方的公钥RP_k进行数字签名并打包成完整确认信息；至此，一条所述权益描述的确认包括了所述权益受益人、所述权益责任人以及所述权益子链三方对权益内容确认；

[0055] 进一步的，所述权益子链每一个时间周期，例如每10分钟或者20分钟，对该段时间内确认过的所有所述权益描述确认信息进行统一收集，并通过共识机制，选取所述权益子链内的其中一个节点作为目标节点，生成所述权益子链的第n个信息区块的区块主体；所述第n个信息区块的区块头内，写入由第n-1个信息区块的所有记录信息通过哈希算法加密后得到的固定长度字段；当后续需要验证所述第n个信息区块的真确性时，则可以通过识别所述第n个信息区块的区块头确认其对之前所有区块的真确性延续；

[0056] 进一步的，所述通证子链在每一次检验并通过后，都生成一个新的区块，记录本次检验中的所有记录信息，包括本次通证验证的所有所述权益描述，以及本次参与验证的所有所述权益子链的确认信息以及参与的所述权益责任方节点的信息；

[0057] 以上为本实施例实现通证交换的过程中对使用者身份的检验方法。

[0058] 实施例二：

[0059] 本实施例应当理解为至少包含前述任一一个实施例的全部特征，并在其基础上进一步改进；一种在通证交换的过程中对使用者身份的检验方法；所述检验方法由通证主链、通证子链以及多条权益子链组成检验过程的参与方；所述通证主链包含通证系统内所有通证的权益信息；所述通证子链包含一个通证的所有权益信息的合集；每条所述权益子链用于验证一项权益；

[0060] 其中，所述通证子链由所述通证主链生成；所述通证子链的第一个区块为创世区块；所述创世区块生成时，由所述通证主链中各节点对所述创世区块写入权益描述；所述权

益描述包括权益受益方信息以及权益的具体内容;所述权益的具体内容至少包括权益责任方、权益执行方式以及时效;所述权益受益方通过所述通证主链各节点验证有效性,并在验证后生成一对代表所述权益受益方的公钥P_k和私钥S_k;所述公钥P_k广播到所述通证主链以及多条所述权益子链,并由所述通证主链以及多条所述权益子链的节点通过哈希加密算法,将确认信息加上所述公钥P_k生成确认回函,并对所述确认回函进行哈希运算后,存储到所述通证子链的所述创世区块的区块头内,所述权益受益方刚可以使用持有的所述私钥S_k验证在所述通证子链区块头内的确认回函的哈希值,用于确认所述权益受益方的身份已经由所述通证主链以及多条所述权益子链所记录并承认;所述通证子链的第二区块在通证进行下一次验证时生成,并通过对所述创世区块的包含的内容进行哈希运算后生成固定长度的字段,作为第二区块的区块头;并且所述通证子链的第n+1个区块生成时,都将所述通证子链的第n个区块进行哈希运算后,生成固定长度的字段作为第n+1个区块的区块头;使用此方法,所述通证子链中的区块具备顺序溯源特性,在今后每次验证通证时,通过验证新区块头的信息确认之前区块的有效性;

[0061] 所述通证主链具有加密通讯接口;所述通证子链以及多条所述权益子链通过所述加密通讯接口与所述通证主链进行通讯;通讯内容包括所述通证子链以及多条所述权益子链对所述通证主链发起广播,以及所述通证子链以及多条所述权益子链接收所述通证主链的区块信息;

[0062] 通证的使用者以所述私钥S_k作为身份凭证确认本人为通证的权益受益人;所述权益受益人使用所述私钥S_k验证在所述通证子链区块头内的确认信息哈希值,用于确认所述权益受益人的身份已经由所述通证主链以及多条所述权益子链所记录并承认;

[0063] 所述通证主链包括一种迭代算法,用于在生成所述通证子链时对通证的所述权益描述进行迭代拆分,直至拆分后每一条所述权益描述只包含一个权益责任方、一个执行方式以及一个执行时效;

[0064] 所述权益子链中包括的每一个所述权益责任方,通过所述通证主链、自身参与的所述权益子链的所有节点认证,并由所述通证主链生成属于所述权益责任方的公钥RP_k和私钥RS_k;

[0065] 所述权益子链采用联盟链形式组建;每条所述权益子链代表一项不可再拆分的权益;所述权益子链中的节点的属性为轻节点;所述权益子链中的节点由所有执行本权益子链代表的权益时涉及的每一个所述权益责任方的节点组成;所述权益子链的联盟链形式,排除所有与所述权益子链无关的节点的参与权限,并且定期执行此排除操作,以确定所述联盟链内的所有节点处于活跃且可工作状态;

[0066] 所述一种在通证交换的过程中对使用者身份的检验方法的检验过程包括以下步骤:

[0067] S1,使用者凭私钥S_k验证所述通证子链的创始区块内的多项身份确认信息,证明所持有的私钥S_k与准备验证的所述通证子链正确配对;

[0068] S2,使用者将需要验证所述通证子链的需求信息向所述通证主链提交广播;

[0069] S3,所述通证主链在收到所述通证子链的广播信息后,将所述通证子链的最后一个区块的每一条所述权益描述向主链上各节点广播;所述通证主链的各节点使用迭代算法验证是否每一条所述权益描述不可以再进行拆分,以及验证每一条所述权益描述是否至少

包括以下信息:权益责任方、权益执行方式以及权益时效;

[0070] S4,所述通证主链根据权益种类对所述通证子链内的每一条所述权益描述进行分类,并按照分类将每一条所述权益描述,通过所述权益受益人的公钥P_k进行数字签名,并加上事件编号,分派到对应的所述权益子链上进行验证;

[0071] S5,所述权益子链上的每一个节点将接收到的每一条所述权益描述进行比对,按照所述权益描述包括的一个权益责任方、一个执行方式以及一个执行时效,所述权益子链的各节点进行确认;所述权益子链的各节点将确认结果在所述权益子链的最后一个区块进行记录;每条所述权益描述由所述权益责任方使用拥有的私钥RS_k进行数字签名;

[0072] S6,在完成一个完整的所述权益子链区块后,将生成的区块广播到所述通证主链;所述通证主链的节点可以使用多个所述权益责任方的公钥RP_k对每一条所述权益描述进行验证;能够通过验证的所述权益描述,即代表已经得到所述权益责任方的确认;

[0073] S7,所述通证主链在接收到属于相同事件编号的一系列广播信息后,生成最新区块的记录信息,统计此事件编号在S3步骤中发送的所有广播信息已经全部得到所有所述权益子链的确认;若是,则通过所述通证子链的验证,并允许使用者对通证作出交换操作;

[0074] 当所述权益子链需要生成第n个所述信息区块时,由于要选取其中一个节点作为生成新区块的目标节点,同时需要考虑选出的所述目标节点可能基于利益,与大于51%数量的其他所述权益子链节点进行串通,对所述权益描述进行非法篡改,因此本实施例执行一种基于各节点投票权重的投票模式进行目标节点的选举;

[0075] 当一个新的区块开启之始,所述权益子链将所有链内节点的权重初始值Q设为1;在获得一条所述权益描述并识别该条所述权益描述的所述权益责任人后,进行一次权重值更新;权重值更新包括以下步骤:

[0076] E1:将所述权益描述中指向的所述权益责任人的权重值不变;

[0077] E2:所述权益子链内其他节点的权重值乘以1.1,即Q=1*1.1=1.1;

[0078] 通过第j条权重描述的识别后,与所有所述权重描述都不相关的节点,其权重值将为$Q=1*1.1^j$;而涉及i个所述权重描述的节点,其权重值为$Q=1*1.1^j$;以此则可以使涉及权重越多的节点,其权重值则越低;

[0079] 进一步的,对于同一事件编号内涉及的两个或以上的所述权益责任方,则同时将该两个或以上的所述权益责任方的权重值都乘以0.9,使所述权益描述可能存在串通的两方或多方的权重值进一步降低;

[0080] 进一步的,统计第n个区块生成周期内所有节点的权重值,选取其中权重最高的10个节点进行随机抽取,选出一个节点作为目标节点生成第n个区块,并将第n个区块广播到所有节点进行验证后,接在所述权益子链的最后,完成第n个区块的生成,并且接着开启第n+1个区块的生成周期。

[0081] 实施例三:

[0082] 本实施例应当理解为至少包含前述任一一个实施例的全部特征,并在其基础上进一步改进:一种在通证交换的过程中对使用者身份的检验方法;所述检验方法由通证主链、通证子链以及多条权益子链组成检验过程的参与方;所述通证主链包含通证系统内所有通证的权益信息;所述通证子链包含一个通证的所有权益信息的合集;每条所述权益子链用

于验证一项权益；

[0083] 其中，所述通证子链由所述通证主链生成；所述通证子链的第一个区块为创世区块；所述创世区块生成时，由所述通证主链中各节点对所述创世区块写入权益描述；所述权益描述包括权益受益方信息以及权益的具体内容；所述权益的具体内容至少包括权益责任方、权益执行方式以及时效；所述权益受益方通过所述通证主链各节点验证有效性，并在验证后生成一对代表所述权益受益方的公钥P_k和私钥S_k；所述公钥P_k广播到所述通证主链以及多条所述权益子链，并由所述通证主链以及多条所述权益子链的节点通过哈希加密算法，将确认信息加上所述公钥P_k生成确认回函，并对所述确认回函进行哈希运算后，存储到所述通证子链的所述创世区块的区块头内，所述权益受益方刚可以使用持有的所述私钥S_k验证在所述通证子链区块头内的确认回函的哈希值，用于确认所述权益受益方的身份已经由所述通证主链以及多条所述权益子链所记录并承认；所述通证子链的第二区块在通证进行下一次验证时生成，并通过对所述创世区块的包含的内容进行哈希运算后生成固定长度的字段，作为第二区块的区块头；并且所述通证子链的第n+1个区块生成时，都将所述通证子链的第n个区块进行哈希运算后，生成固定长度的字段作为第n+1个区块的区块头；使用此方法，所述通证子链中的区块具备顺序溯源特性，在今后每次验证通证时，通过验证新区块头的信息确认之前区块的有效性；

[0084] 所述通证主链具有加密通讯接口；所述通证子链以及多条所述权益子链通过所述加密通讯接口与所述通证主链进行通讯；通讯内容包括所述通证子链以及多条所述权益子链对所述通证主链发起广播，以及所述通证子链以及多条所述权益子链接收所述通证主链的区块信息；

[0085] 通证的使用者以所述私钥S_k作为身份凭证确认本人为通证的权益受益人；所述权益受益人使用所述私钥S_k验证在所述通证子链区块头内的确认信息哈希值，用于确认所述权益受益人的身份已经由所述通证主链以及多条所述权益子链所记录并承认；

[0086] 所述通证主链包括一种迭代算法，用于在生成所述通证子链时对通证的所述权益描述进行迭代拆分，直至拆分后每一条所述权益描述只包含一个权益责任方、一个执行方式以及一个执行时效；

[0087] 所述权益子链中包括的每一个所述权益责任方，通过所述通证主链、自身参与的所述权益子链的所有节点认证，并由所述通证主链生成属于所述权益责任方的公钥RP_k和私钥RS_k；

[0088] 所述权益子链采用联盟链形式组建；每条所述权益子链代表一项不可再拆分的权益；所述权益子链中的节点的属性为轻节点；所述权益子链中的节点由所有执行本权益子链代表的权益时涉及的每一个所述权益责任方的节点组成；所述权益子链的联盟链形式，排除所有与所述权益子链无关的节点的参与权限，并且定期执行此排除操作，以确定所述联盟链内的所有节点处于活跃且可工作状态；

[0089] 所述一种在通证交换的过程中对使用者身份的检验方法的检验过程包括以下步骤：

[0090] S1，使用者凭私钥S_k验证所述通证子链的创始区块内的多项身份确认信息，证明所持有的私钥S_k与准备验证的所述通证子链正确配对；

[0091] S2，使用者将需要验证所述通证子链的需求信息向所述通证主链提交广播；

[0092] S3,所述通证主链在收到所述通证子链的广播信息后,将所述通证子链的最后一个区块的每一条所述权益描述向主链上各节点广播;所述通证主链的各节点使用迭代算法验证是否每一条所述权益描述不可以再进行拆分,以及验证每一条所述权益描述是否至少包括以下信息:权益责任方、权益执行方式以及权益时效;

[0093] S4,所述通证主链根据权益种类对所述通证子链内的每一条所述权益描述进行分类,并按照分类将每一条所述权益描述,通过所述权益受益人的公钥P_k进行数字签名,并加上事件编号,分派到对应的所述权益子链上进行验证;

[0094] S5,所述权益子链上的每一个节点将接收到的每一条所述权益描述进行比对,按照所述权益描述包括的一个权益责任方、一个执行方式以及一个执行时效,所述权益子链的各节点进行确认;所述权益子链的各节点将确认结果在所述权益子链的最后一个区块进行记录;每条所述权益描述由所述权益责任方使用拥有的私钥RS_k进行数字签名;

[0095] S6,在完成一个完整的所述权益子链区块后,将生成的区块广播到所述通证主链;所述通证主链的节点可以使用多个所述权益责任方的公钥RP_k对每一条所述权益描述进行验证;能够通过验证的所述权益描述,即代表已经得到所述权益责任方的确认;

[0096] S7,所述通证主链在接收到属于相同事件编号的一系列广播信息后,生成最新区块的记录信息,统计此事件编号在S3步骤中发送的所有广播信息已经全部得到所有所述权益子链的确认;若是,则通过所述通证子链的验证,并允许使用者对通证作出交换操作;

[0097] 本实施例中,各所述权益子链的联盟链内存在节点的数量可能存在较大差异;部分所述权益子链中代表的权益种类有可能使用频率不高,导致拥有验证资格的节点太少,最终使这些联盟链内存在类中心化的验证环境,不利于所述权益子链负责的权益的公平验证;本实施例针对个别所述权益子链中,验证节点数量太少的缺陷,改进本发明的检验方法;

[0098] 所述通证主链在建设白皮中,应该根据实验室计算权益验证最低验证节点数量的模形,设定每个所述权益子链至少拥有的有效节点阈值η;通证在所述通证主链进行权益分拆后,所述通证主链对通证涉及的多个所述权益子链进行有效节点统计;对低于所述有效节点阈值η的所述权益子链进行广播,提出临时增加验证节点的要求;

[0099] 临时选定的节点,使用一种历史验证通证数量的统计分析,对所述通证主链内的节点进行选择;所述通证主链对每次有通证进行上链验证时,都对当前链上具备工作能力并且可以作出验证功能的节点进行记名统计,对作出统计列表,例如:<通证编号,{验证节点集合}>,并且该列表信息进行所述通证主链上的全链验证后,加入所述通证主链的区块信息中;所述通证主链的区块信息会一直保留在历史过程中,其中就包括每一个通证进行过有效通证验证的节点的所有统计信息;而无效的验证节点或者验证结果,由于区块链的唯一性原则,必然已被删除并且不会计入统计次数;因此,通过统计所述通证主链中所有有效点节中,进行过有效验证次数最多的i个节点,并记录这些节点的公钥组成集合$Temp\{Pt\}=\{Pt_1,Pt_2\cdots\cdots Pt_i\}$; 由于该部分在所述通证主链中验证次数较多的节点,其工作量以及验证可信度都较高,可以作为一种链上的“验证权益抵押”,以此证明其自身的信度程度和可靠程度;

[0100] 进一步的,根据所述权益子链的节点数量缺口,进行随机抽取节点,从集合$Temp\{Pt\}$中抽取若干个节点,加入所述多个所述权益子链的联盟链中,并向联盟链中的当前节

点发出广播要求验证并记录该部分临时节点；

[0101] 进一步的，若被指派临时节点的联盟链一致通过所有临时增加的节点，刚进行所述检验方法的正常实施；若被指派临时节点的联盟链不能一致通过增加临时节点，则可以由所述通证主链再次抽取Temp{Pt}的节点重新广播。

[0102] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0103] 虽然上面已经参考各种实施例描述了本发明，但是应当理解，在不脱离本发明的范围的情况下，可以进行许多改变和修改。也就是说上面讨论的方法，系统和设备是示例。各种配置可以适当地省略，替换或添加各种过程或组件。例如，在替代配置中，可以以与所描述的顺序不同的顺序执行方法，和/或可以添加，省略和/或组合各种部件。而且，关于某些配置描述的特征可以以各种其他配置组合，如可以以类似的方式组合配置的不同方面和元素。此外，随着技术发展其中的元素可以更新，即许多元素是示例，并不限制本公开或权利要求的范围。

[0104] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而，可以在没有这些具体细节的情况下实践配置例如，已经示出了众所周知的电路，过程，算法，结构和技术而没有不必要的细节，以避免模糊配置。该描述仅提供示例配置，并且不限制权利要求的范围，适用性或配置。相反，前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下，可以对元件的功能和布置进行各种改变。

[0105] 综上，其旨在上述详细描述被认为是例示性的而非限制性的，并且应当理解，以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后，技术人员可以对本发明作各种改动或修改，这些等效变化和修饰同样落入本发明权利要求所限定的范围。

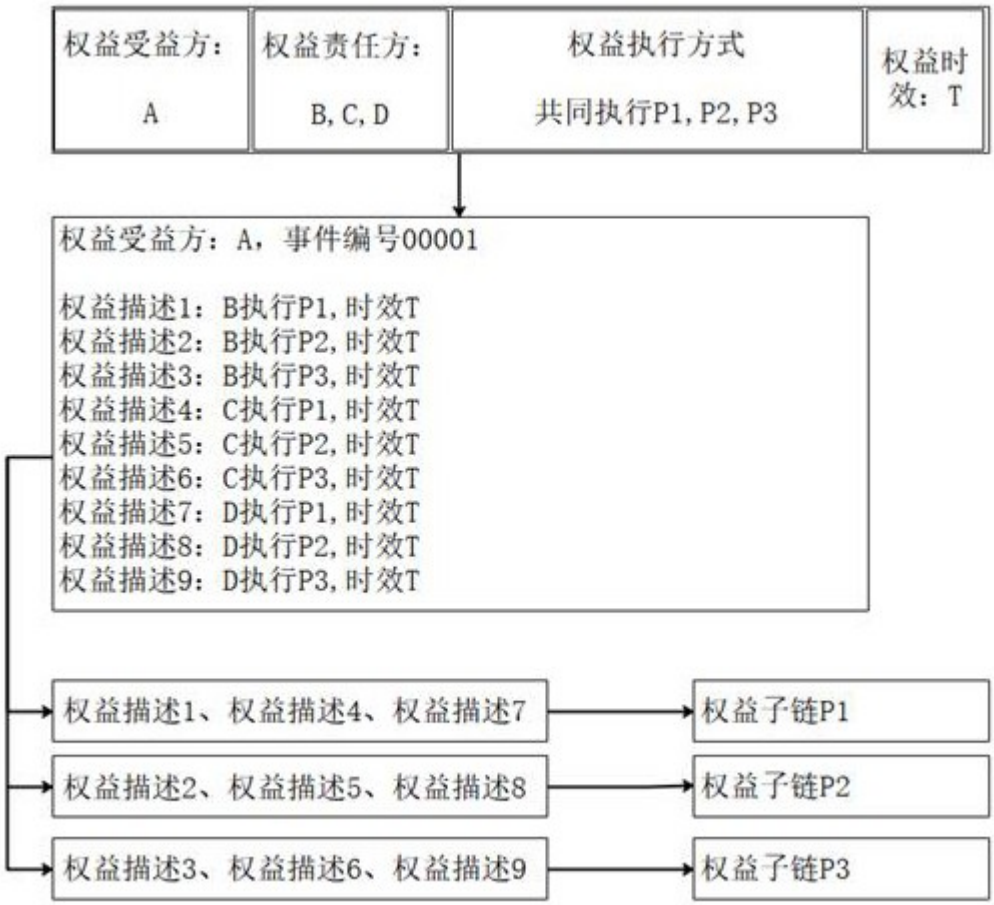

权益受益方：
A
权益责任方：
B, C, D
权益执行方式
共同执行P1, P2, P3
权益时效：T
权益受益方：A，事件编号00001
权益描述1：B执行P1, 时效T
权益描述2：B执行P2, 时效T
权益描述3：B执行P3, 时效T
权益描述4：C执行P1, 时效T
权益描述5：C执行P2, 时效T
权益描述6：C执行P3, 时效T
权益描述7：D执行P1, 时效T
权益描述8：D执行P2, 时效T
权益描述9：D执行P3, 时效T
权益描述1、权益描述4、权益描述7
权益子链P1
权益描述2、权益描述5、权益描述8
权益子链P2
权益描述3、权益描述6、权益描述9
权益子链P3

图1

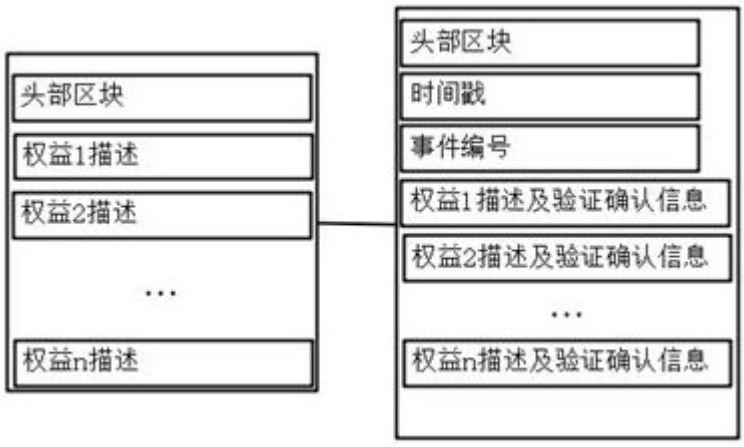

头部区块
权益1描述
权益2描述
...
权益n描述
头部区块
时间戳
事件编号
权益1描述及验证确认信息
权益2描述及验证确认信息
...
权益n描述及验证确认信息

图2

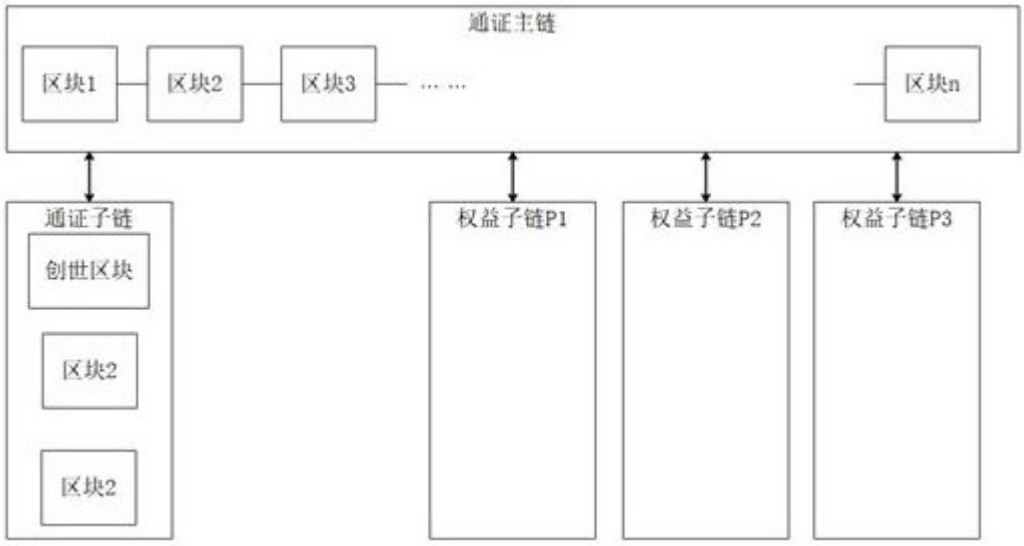


图3