(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 113660294 B
(45)授权公告日 2021.12.14

(21)申请号 202111218894.8
(22)申请日 2021.10.20
(65)同一申请的已公布的文献号
申请公布号 CN 113660294 A
(43)申请公布日 2021.11.16
(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 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.
H04L 29/06(2006.01)
G06Q 20/04(2012.01)

(56)对比文件
CN 111669268 A,2020.09.15
CN 109086601 A,2018.12.25
US 2020320488 A1,2020.10.08
US 2020084023 A1,2020.03.12
WO 2021112746 A1,2021.06.10
CN 109274496 A,2019.01.25
Bjorn Tackmann.Secure Event Tickets on a Blockchain.《DPM/CBT 2017》.2017,
Hongkai Wang.Design of Work Ticket System and Scheduling Algorithm based on Blockchain.《2020 IEEE Symposium Series on Computational Intelligence》.2021,
牛杰.区块链算法在物联网中的应用研究.《中国优秀硕士学位论文全文数据库 (信息科技辑)》.2021,
靳世雄.区块链共识算法研究综述.《信息安全学报》.2021,第6卷(第2期),

审查员 李炯

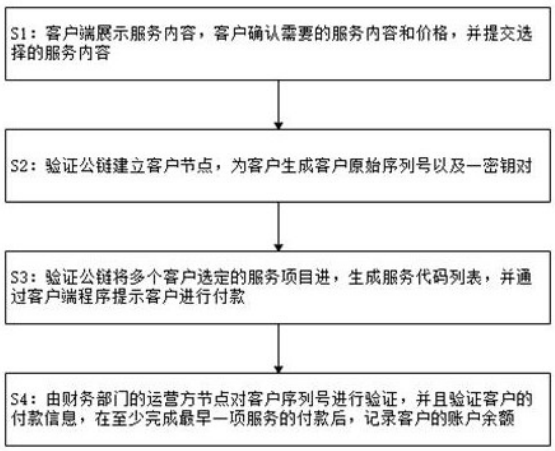
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种非对称加密模式下的票序列号核验方法

(57)摘要

本发明提供了一种非对称加密模式下的票序列号核验方法;所述核验方法运行于一个验证区块链主链上,客户以及多个运营方作为所述验证主链上的节点;客户节点对自身信息进行非对称加密获得加密序列号从而用于身份认证;服务部门节点对客户需求的多项服务项目进行验证并进行非对称加密后获得多个加密服务序列号;在兑现服务时,通过按时间排序的方式,由服务部门节点验证所述加密服务序列号并要求客户验证其身份信息,并计算客户账户余额后,才正式兑现服务,实现服务项目的唯一性实现以及多次验证,确保服务运营商的效益最大化。



CN 113660294 B

1.一种非对称加密模式下的票券序列号核验方法,其特征在于,所述核验方法在一条验证公链上进行;由票券包含的所有权益方作为所述验证公链上的所有节点对所述验证公链上的区块信息进行一致性共识认证;所述节点中包括由多个客户组成的客户节点;所述客户节点为临时性节点;所述客户节点的有效时间从客户提交购票需求开始,直到票券的权益被全部兑现后结束;所述节点中还包括多个运营节点;所述运营节点包括提供服务的服务部门节点以及负责核销的会计节点;所述运营节点为常驻节点,每个所述验证公链上的区块的验证都必须获得每个所述运营节点的参与;

其中,所述验证公链上的每个节点在成为有效节点后,由所述验证公链生成一对代表该节点的公钥Pk和私钥Sk;所述公钥Pk和所述私钥Sk由非对称加密算法生成;每个节点的所述公钥Pk在生成后统一公开并广播到所述验证公链全链;所述私钥Sk由各节点保管并自行保密;客户在确定需要的服务项目内容后,将确认结果广播到所述验证公链后生成服务代码列表,并由多个所述运营节点将所述服务代码列表内的服务项目逐一验证;验证时,由所述服务部门节点使用自身的所述公钥Pk,对所述服务代码列表内属于其运营的服务项目加上客户当前拥有的加密序列号后,进行非对称加密,从而将服务代码列表内的多个服务项目形成多个与客户相关联的加密服务序列号;所述服务代码列表挂载于所述客户节点下,并且每个客户节点在同一时刻最多挂载一份所述服务代码列表。

2.根据权利要求1所述一种非对称加密模式下的票券序列号核验方法,其特征在于,所述验证公链具有应用程序接口;外部客户端应用程序通过所述应用程序接口,与所述验证公链进行数据交换。

3.根据权利要求2所述一种非对称加密模式下的票券序列号核验方法,其特征在于,所述客户端应用程序用于展示运营方能够提供的每一项服务的相关资讯给予客户选择;客户在选择至少一项的服务后,由所述客户端应用程序向所述验证公链提交购买服务需求;在服务需求提交后,所述验证公链接入客户的身份信息,为客户建立所述客户节点。

4.根据权利要求3所述一种非对称加密模式下的票券序列号核验方法,其特征在于,在所述验证公链验证每个客户的身份信息后生成客户原始序列号,并发送到对应的所述客户节点;所述客户原始序列号为固定长度的随机序列纯数字型字符串。

5.根据权利要求4所述一种非对称加密模式下的票券序列号核验方法,其特征在于,客户使用所述客户节点对选择的服务项目进行一次性或分次付款;款项将由所述客户节点向所述会计节点进行转账;转账信息由所述会计节点进行打包到所述验证公链的最新区块内,并由所述验证公链上所有节点进行验证;在获得所有节点的验证后,客户的账户余额与所述客户原始序列号进行绑定,并由所述会计节点通过所述客户节点的客户公钥Pk,生成第一加密序列号,并将所述第一加密序列号返回给所述客户节点。

6.根据权利要求5所述一种非对称加密模式下的票券序列号核验方法,其特征在于,每一项服务项目都具有一个固定字节长度的服务代码;每一项所述服务代码包括服务特征码Sc、服务时间信息St以及服务价格信息Sp;每一项所述服务代码都由一个所述服务部门负责提供服务;所述服务代码在所述验证公链上获得全部节点的一致性共识承认。

7.根据权利要求6所述一种非对称加密模式下的票券序列号核验方法,其特征在于,所述服务时间信息St包括服务开始时间T_s以及服务持续时间T_c;所述服务价格信息Sp与所述服务开始时间T_s以及所述服务持续时间T_c相关;所述服务时间信息St以及所述服务价格信

息Sp是指定长度和格式的字符串;所述服务开始时间T_s额外添加写入在所述加密服务序列号外。

8.根据权利要求7所述一种非对称加密模式下的票券序列号核验方法,其特征在于,客户通过所述客户端应用程序选定具体需要兑现的服务项目,向所述验证公链发出兑现需求;所述验证公链接收到兑现需求后,读取所述客户节点下的所述服务代码列表,并按照所述服务开始时间T_s对多条所述加密服务序列号进行排序;通过所述客户端应用程序的映射,筛选出客户选定的服务项目对应的所述加密服务序列号,并将其余未被选中的服务项目对应的所述加密服务序列号列为非可读;所述验证公链广播所述服务代码列表,所有所述服务部门节点使用自身的所述私钥Sk,按所述服务开始时间T_s的最近次序,验证所述服务代码列表中当前可读的所述加密服务序列号;并在其中一个所述服务部门节点正确解密后停止所述服务代码列表的广播。

9.根据权利要求8所述一种非对称加密模式下的票券序列号核验方法,其特征在于,成功解密的所述服务部门节点对解密后的所述服务代码进行解析,并按照所述服务时间信息St以及所述服务价格信息Sp计算服务项目应该扣除的服务金额;并将上述解析结果广播到所述验证公链;所述验证公链收到所述解析结果后,要求所述客户节点通过自身的私钥Sk解密所述第一加密序列号后,计算所述账户余额是否大于所述服务金额,并在确认可以扣除后,广播扣除余额信息到所述验证公链。

10.根据权利要求9所述一种非对称加密模式下的票券序列号核验方法,其特征在于,所述验证公链根据所述服务金额扣除所述客户节点的余额,由所述会计节点使用所述客户公钥Pk重新加密解密后的所述第一加密序列号,得到第二加密序列号;所述验证公链将所述服务列表内被解密的所述服务项目清除,并要求所有所述服务部门节点解密其余所述服务项目后,基于所述第二加密序列号,重新加密余下的所有服务项目,生成多项第二加密服务序列号,挂载到所述客户节点下的所述服务代码列表。

一种非对称加密模式下的票序列号核验方法

技术领域

[0001] 本发明涉及公共票务核验技术领域。具体而言，涉及一种非对称加密模式下的票序列号核验方法。

背景技术

[0002] 随着当前大型活动场所或者大型群众活动的大量举办，对于票务系统提出了新的要求。在一场大型活动或者一个举办大型活动的场地中，存在着多个需要单个购票的活动项目，并且每个活动项目每日都有不固定的场次以及举行的时间段。因此要参与活动的参与者来说，则需要分别选择项目、场次、时间、价格等信息，并需要保存数个购票凭证，以证明其权益。

[0003] 进一步的，存在参加者购买的场次与实际参与的场次不符，或者少买、漏买场次，以低价场次冒充高价场次的手段进行欺骗。主办方为保证票务的最大收益，则需要对多个场次的每一个参与者都进行验票，相关的工作量大，容易出错；而且服务体验不好，对参加者或者主办方来说都存在服务质量可提升的空间。

[0004] 查阅相关地已公开技术方案，公开号为US2021272026A1提出一种票务系统，该票务系统发行的票券直接记录购票人对活动场次、对应价格阶段的选定，而并非在购买时直接记录于系统内，用于节省处理票务数据的服务器资源；公开号CN212624158 (U) 的技术方案提出通过大数据技术应用的多功能智慧票务系统，从而杜绝第三方人员对票据作假、恶意屯票、非法炒高价格等恶劣行为；公开号为TW201928849 (A) 的技术方案提出一种适用于自由式音乐会的可针对退票后的票据再次释放的票务系统，提高票据在二次销售效率。然而当前方案主要针对销售与管理过程，少有涉及对于多场景应用的单一票据的验证方案。

发明内容

[0005] 本发明的目的在于，提供一种非对称加密模式下的票序列号核验方法；所述核验方法利用非对称加密的算法对于加密的运算速度快、运算成本低，而破解难、成本高的特点，对需要进行多场次验票的场景进行多级加密，提高购票验票的效率，也提升整体的服务感受。

[0006] 本发明采用如下技术方案：

[0007] 一种非对称加密模式下的票券序列号核验方法，其特征在于，所述核验方法在一条验证公链上进行；由票券包含的所有权益方作为所述验证公链上的所有节点对所述验证公链上的区块信息进行一致性共识认证；所述节点中包括由多个客户组成的客户节点；所述客户节点为临时性节点；所述客户节点的有效时间从客户提交购票需求开始，直到票券的权益被全部兑现后结束；所述节点中还包括多个运营节点；所述运营节点包括提供服务的服务部门节点以及负责核销的会计节点；所述运营节点为常驻节点，每个所述验证公链上的区块的验证都必须获得每个所述运营节点的参与；

[0008] 其中，所述验证公链上的每个节点在成为有效节点后，由所述验证公链生成一对代表该节点的公钥Pk和私钥Sk；所述公钥Pk和所述私钥Sk由非对称加密算法生成；每个节点的所述公钥Pk在生成后统一公开并广播到所述验证公链全链；所述私钥Sk由各节点保管并自行保密；客户在确定需要的服务项目内容后，将确认结果广播到所述验证公链后生成服务代码列表，并由多个所述运营节点将所述服务代码列表内的服务项目逐一验证；验证时，由所述服务部门节点使用自身的所述公钥Pk，对所述服务代码列表内属于其运营的服务项目加上客户当前拥有的加密序列号后，进行非对称加密，从而将服务代码列表内的多个服务项目形成多个与客户相关联的加密服务序列号；所述服务代码列表挂载于所述客户节点下，并且每个客户节点在同一时刻最多挂载一份所述服务代码列表；

[0009] 所述验证公链具有应用程序接口；外部客户端应用程序通过所述应用程序接口，与所述验证公链进行数据交换；

[0010] 所述客户端应用程序用于展示运营方能够提供的每一项服务的相关资讯给予客户选择；客户在选择至少一项的服务后，由所述客户端应用程序向所述验证公链提交购买服务需求；在服务需求提交后，所述验证公链接入客户的身份信息，为客户建立所述客户节点；

[0011] 在所述验证公链验证每个客户的身份信息后生成客户原始序列号，并发送到对应的所述客户节点；所述客户原始序列号为固定长度的随机序列纯数字型字符串；

[0012] 客户使用所述客户节点对选择的服务项目进行一次性或分次付款；款项将由所述客户节点向所述会计节点进行转账；转账信息由所述会计节点进行打包到所述验证公链的最新区块内，并由所述验证公链上所有节点进行验证；在获得所有节点的验证后，客户的账户余额与所述客户原始序列号进行绑定，并由所述会计节点通过所述客户节点的客户公钥Pk，生成第一加密序列号，并将所述第一加密序列号返回给所述客户节点；

[0013] 每一项服务项目都具有一个固定字节长度的服务代码；每一项所述服务代码包括服务特征码Sc、服务时间信息St以及服务价格信息Sp；每一项所述服务代码都由一个所述服务部门负责提供服务；所述服务代码在所述验证公链上获得全部节点的一致性共识承认；

[0014] 所述服务时间信息St包括服务开始时间T_s以及服务持续时间T_c；所述服务价格信息Sp与所述服务开始时间T_s以及所述服务持续时间T_c相关；所述服务时间信息St以及所述服务价格信息Sp是指定长度和格式的字符串；所述服务开始时间T_s额外添加写入在所述加密服务序列号外；

[0015] 客户通过所述客户端应用程序选定具体需要兑现的服务项目，向所述验证公链发出兑现需求；所述验证公链接收到兑现需求后，读取所述客户节点下的所述服务代码列表，并按照所述服务开始时间T_s对多条所述加密服务序列号进行排序；通过所述客户端应用程序的映射，筛选出客户选定的服务项目对应的所述加密服务序列号，并将其余未被选中的服务项目对应的所述加密服务序列号列为非可读；所述验证公链广播所述服务代码列表，所有所述服务部门节点使用自身的所述私钥Sk，按所述服务开始时间T_s的最近次序，验证所述服务代码列表中当前可读的所述加密服务序列号；并在其中一个所述服务部门节点正确解密后停止所述服务代码列表的广播；

[0016] 成功解密的所述服务部门节点对解密后的所述服务代码进行解析，并按照所述服

务时间信息St以及所述服务价格信息Sp计算服务项目应该扣除的服务金额;并将上述解析结果广播到所述验证公链;所述验证公链收到所述解析结果后,要求所述客户节点通过自身的私钥Sk解密所述第一加密序列号后,计算所述账户余额是否大于所述服务金额,并在确认可以扣除后,广播扣除余额信息到所述验证公链;

[0017] 所述验证公链根据所述服务金额扣除所述客户节点的余额,由所述会计节点使用所述客户公钥Pk重新加密解密后的所述第一加密序列号,得到第二加密序列号;所述验证公链将所述服务列表内被解密的所述服务项目清除,并要求所有所述服务部门节点解密其余所述服务项目后,基于所述第二加密序列号,重新加密余下的所有服务项目,生成多项第二加密服务序列号,挂载到所述客户节点下的所述服务代码列表。

[0018] 本发明所取得的有益效果是:

[0019] 1.本发明的核验方法通过将客户的信息进行数字化整理,生成随机的序列号,并且将客户的余额信息通过会计节点的非对称加密方法,使客户本身的身份与余额信息都被足够混淆,有效避免了服务节点对特别客户的特殊对待,保护了运营方的利益;

[0020] 2.本发明的核验方法的所有信息,包括付款信息,生成余额信息,扣除款项信息,服务兑现信息都通过区块链的共识制度以及全链记录制度进行一致性验证,使用了全链多个节点的信用背书。

[0021] 3.本发明的核验方法支持将客户的需求服务细分为多项,并由多个服务责任方进行各自单独的验证,将验证的义务分散到各个服务方,减低了主运营方的验证和成本负担。

[0022] 4.本发明的核验方法对软、硬件模块化设计,方便今后的升级或者更换相关的软、硬件环境,降低了使用的成本。

附图说明

[0023] 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。

[0024] 图1为本发明中所述客户节点的生成流程示意图;

[0025] 图2为本发明所述服务代码中的构成示意图;

[0026] 图3为本发明所述服务代码列表的生成流程示意图;

[0027] 图4为本发明客户选定所需服务项目的票务生成流程示意图;

[0028] 图5为本发明客户选定所需兑现的服务项目的票务验证流程示意图。

具体实施方式

[0029] 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。

[0030] 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。

[0031] 实施例一：

[0032] 一种非对称加密模式下的票券序列号核验方法，其特征在于，所述核验方法在一条验证公链上进行；由票券包含的所有权益方作为所述验证公链上的所有节点对所述验证公链上的区块信息进行一致性共识认证；所述节点中包括由多个客户组成的客户节点；所述客户节点为临时性节点；所述客户节点的有效时间从客户提交购票需求开始，直到票券的权益被全部兑现后结束；所述节点中还包括多个运营节点；所述运营节点包括提供服务的服务部门节点以及负责核销的会计节点；所述运营节点为常驻节点，每个所述验证公链上的区块的验证都必须获得每个所述运营节点的参与；

[0033] 其中，所述验证公链上的每个节点在成为有效节点后，由所述验证公链生成一对代表该节点的公钥Pk和私钥Sk；所述公钥Pk和所述私钥Sk由非对称加密算法生成；每个节点的所述公钥Pk在生成后统一公开并广播到所述验证公链全链；所述私钥Sk由各节点保管并自行保密；客户在确定需要的服务项目内容后，将确认结果广播到所述验证公链后生成服务代码列表，并由多个所述运营节点将所述服务代码列表内的服务项目逐一验证；验证时，由所述服务部门节点使用自身的所述公钥Pk，对所述服务代码列表内属于其运营的服务项目加上客户当前拥有的加密序列号后，进行非对称加密，从而将服务代码列表内的多个服务项目形成多个与客户相关联的加密服务序列号；所述服务代码列表挂载于所述客户节点下，并且每个客户节点在同一时刻最多挂载一份所述服务代码列表；

[0034] 所述验证公链具有应用程序接口；外部客户端应用程序通过所述应用程序接口，与所述验证公链进行数据交换；

[0035] 所述客户端应用程序用于展示运营方能够提供的每一项服务的相关资讯给予客户选择；客户在选择至少一项的服务后，由所述客户端应用程序向所述验证公链提交购买服务需求；在服务需求提交后，所述验证公链接入客户的身份信息，为客户建立所述客户节点；

[0036] 在所述验证公链验证每个客户的身份信息后生成客户原始序列号，并发送到对应的所述客户节点；所述客户原始序列号为固定长度的随机序列纯数字型字符串；

[0037] 客户使用所述客户节点对选择的服务项目进行一次性或分次付款；款项将由所述客户节点向所述会计节点进行转账；转账信息由所述会计节点进行打包到所述验证公链的最新区块内，并由所述验证公链上所有节点进行验证；在获得所有节点的验证后，客户的账户余额与所述客户原始序列号进行绑定，并由所述会计节点通过所述客户节点的客户公钥Pk，生成第一加密序列号，并将所述第一加密序列号返回给所述客户节点；

[0038] 每一项服务项目都具有一个固定字节长度的服务代码；每一项所述服务代码包括服务特征码Sc、服务时间信息St以及服务价格信息Sp；每一项所述服务代码都由一个所述服务部门负责提供服务；所述服务代码在所述验证公链上获得全部节点的一致性共识承认；

[0039] 所述服务时间信息St包括服务开始时间T_s以及服务持续时间T_c;所述服务价格信息Sp与所述服务开始时间T_s以及所述服务持续时间T_c相关;所述服务时间信息St以及所述服务价格信息Sp是指定长度和格式的字符串;所述服务开始时间T_s额外添加写入在所述加密服务序列号外;

[0040] 客户通过所述客户端应用程序选定具体需要兑现的服务项目,向所述验证公链发出兑现需求;所述验证公链接收到兑现需求后,读取所述客户节点下的所述服务代码列表,并按照所述服务开始时间T_s对多条所述加密服务序列号进行排序;通过所述客户端应用程序的映射,筛选出客户选定的服务项目对应的所述加密服务序列号,并将其余未被选中的服务项目对应的所述加密服务序列号列为非可读;所述验证公链广播所述服务代码列表,所有所述服务部门节点使用自身的所述私钥Sk,按所述服务开始时间T_s的最近次序,验证所述服务代码列表中当前可读的所述加密服务序列号;并在其中一个所述服务部门节点正确解密后停止所述服务代码列表的广播;

[0041] 成功解密的所述服务部门节点对解密后的所述服务代码进行解析,并按照所述服务时间信息St以及所述服务价格信息Sp计算服务项目应该扣除的服务金额;并将上述解析结果广播到所述验证公链;所述验证公链收到所述解析结果后,要求所述客户节点通过自身的私钥Sk解密所述第一加密序列号后,计算所述账户余额是否大于所述服务金额,并在确认可以扣除后,广播扣除余额信息到所述验证公链;

[0042] 所述验证公链根据所述服务金额扣除所述客户节点的余额,由所述会计节点使用所述客户公钥Pk重新加密解密后的所述第一加密序列号,得到第二加密序列号;所述验证公链将所述服务列表内被解密的所述服务项目清除,并要求所有所述服务部门节点解密其余所述服务项目后,基于所述第二加密序列号,重新加密余下的所有服务项目,生成多项第二加密服务序列号,挂载到所述客户节点下的所述服务代码列表;

[0043] 在客户每次完成一个服务项目的况现后,所述验证公链的全链重复以上加密-验证-解密的过程,生成一个全新的所述服务代码列表;

[0044] 由以上实施例可知,客户在每次兑现服务时,都由所有所述服务节点进行所述服务列表的验证,确保客户当前指定的服务项目以及服务项目的信息都可以被负责该服务项目的节点正确验证并承认;进一步的,每个所述服务节点都承担各有验证的责任,并且承担由于错误的价格、服务时间等相关信息的设置错误所带来的经济损失。

[0045] 实施例二:

[0046] 本实施例应当理解为至少包含前述任意一个实施例的全部特征,并在其基础上进一步改进;

[0047] 在某些实施情况中,客户会由于主观或客观的原因,希望更改兑现服务的时间,或者更改已选定的服务项目;而在一些实施情况中,客户无理由地对选定的服务项目放弃兑现其服务权益;由于时间、项目的更改,可能在一定程度上,影响了运营方既定的服务次序安排,导致了一定的运营成本上升,因此在本实施例中,进一步优化本实施方案;

[0048] 客户可通过所述客户端应用程序,在所述服务开始时间T_s的一定时间前,例如30分钟或者60分钟前,向系统提出需要修改例如服务项目、服务时间等相关需求;所述客户端应用程序将客户提出的修改需求提交到所述验证公链;

[0049] 进一步的,当客户在每次通过所述客户端应用程序向所述验证公链提出任何请求

时，所述验证公链则首先验证该客户的所述客户节点下挂载的所述服务代码列表；快速查找其中是否存在所述服务开始时间T_s已超过当前约定服务时间的服务项目；若有，则将超时的所述加密服务序列号进行冻结，并将超时的所述加密服务序列号进行全链广播，将其优化级列为次优先，避免占用当前所述服务节点的验证算力；等待所述验证公链的所述服务节点在空闲时对超时的所述加密服务序列号进行解密，并由最终成功解密的所述服务节点根据超时的所述加密服务序列号包含的所述服务时间信息St以及所述服务价格信息Sp计算服务项目应该扣除的服务金额，并在对应的所述客户节点下，按照惩罚性比例执行余额的扣取，例如按照服务金额的60%或者70%进行扣除，以提醒客户根据约定兑现服务，同时也可以保证服务运营商的利益；

[0050] 进一步的，若在客户提前新的服务需求时，所述服务代码列表并没有超时的服务项目，则由验证公链对需要修改服务需求的原服务项目进行定位，冻结原服务项目的所述加密服务序列号并提出删除验证，同时匹配所述客户节点当前的所述加密序列号，以及新的所述服务特征码Sc、所述服务时间信息St以及所述服务价格信息Sp，通过所述服务节点进行非对称加密后，生成新的所述加密服务序列号，并写入所述服务代码列表，并其所述服务代码列表重新挂载到所述客户节点下。

[0051] 实施例三：

[0052] 本实施例应当理解为至少包含前述任意一个实施例的全部特征，并在其基础上进一步改进：

[0053] 若所述客户节点的所述服务代码列表积压太多服务项目，会对所述运营商的运营效率造成一定的损耗，而保持所述服务代码列表的精简则有利于票务系统的整体运行效率以及加密/解密效率：

[0054] 1．每次对所述服务代码列表进行全体验证时，可能需要验证大量的所述加密服务序列号，并且当中可能存在未超时的以及已经超时的；

[0055] 2．票证在被客户预订后，运营商为保证服务质量，需要预留服务余量给已订票客户，造成服务余量的下降；

[0056] 3．加快消耗所述客户节点下的余额，有利于运营商尽快回笼资金进行周转；

[0057] 因此本实例施针对本技术方案作进一步优化；

[0058] 所述验证公链与每一个所述客户节点约定一个序列号整理时段；所述序列号整理时段以周期性每周，或每两周进行一次；执行所述序列号整理时段的时间通过统计所述服务开始时间T_s找出其中拥有最少服务项目的时间段；

[0059] 进一步的，在所述序列号整理时段中，所述验证公链与所述客户节点同时上链，并针对所述客户节点中的所述服务代码列表进行审阅，对其中的每一条所述加密服务序列号进行共同验证，目的在于：

[0060] 1．通过由所述客户节点，验证是否存在不属于本人的所述加密服务序列号；

[0061] 2．通过所述客户节点解密后的所述服务代码，由客户重新确认是否还需要当前的服务项目，并由客户端应用程序向客户反馈已经服务项目，通过应用程序界面提醒客户；

[0062] 3．统计是否存在服务项目变更，使得存在无法通过非对称解密的所述加密服务序列号；这种情况可能是由于运营商的服务变更导致所述服务节点的密钥对已经更新，从而无法解开过往的加密序列号，当遇到该情况时应由所述验证公链进行全链公投作出共识

性投票，是否删除其中无法解密的所述加密服务序列号；

[0063] 4．若所述服务代码列表的全部所述加密服务序列号都可以进行正确解密，则由所述验证公链统计该份所述服务代码列表包含的所有权益的各个所述服务时间信息St，从而对各个服务项目进行时间序列上的优化，提高运营商本身的运营效率。

[0064] 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。

[0065] 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。

[0066] 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。

[0067] 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。

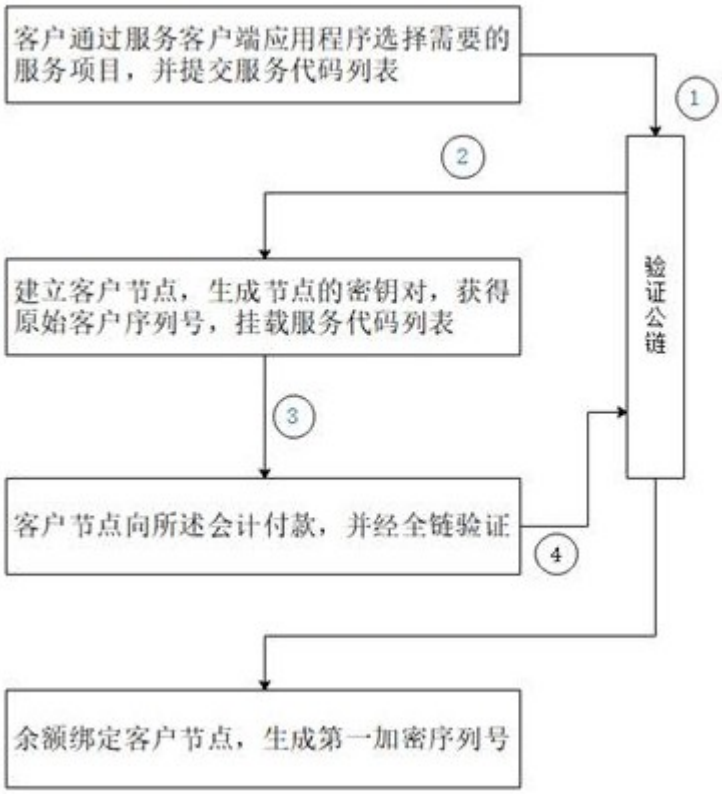

客户通过服务客户端应用程序选择需要的服务项目，并提交服务代码列表
1
2
建立客户节点，生成节点的密钥对，获得原始客户序列号，挂载服务代码列表
验证公链
3
客户节点向所述会计付款，并经全链验证
4
余额绑定客户节点，生成第一加密序列号

图1


服务代码
服务特征码Sc
服务时间信息St
服务价格信息Sp

图2

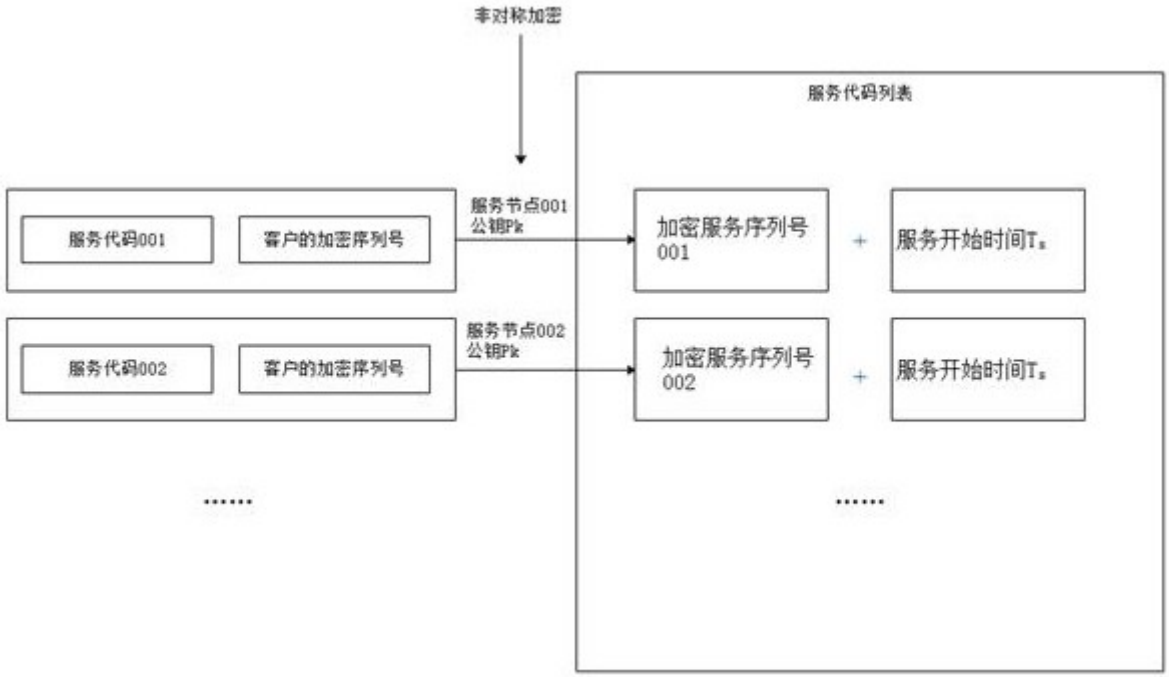

非对称加密
服务代码列表
服务代码001
客户的加密序列号
服务节点001
公钥Pk
加密服务序列号
001
+
服务开始时间T。
服务代码002
客户的加密序列号
服务节点002
公钥Pk
加密服务序列号
002
+
服务开始时间T。
.....
.....

图3

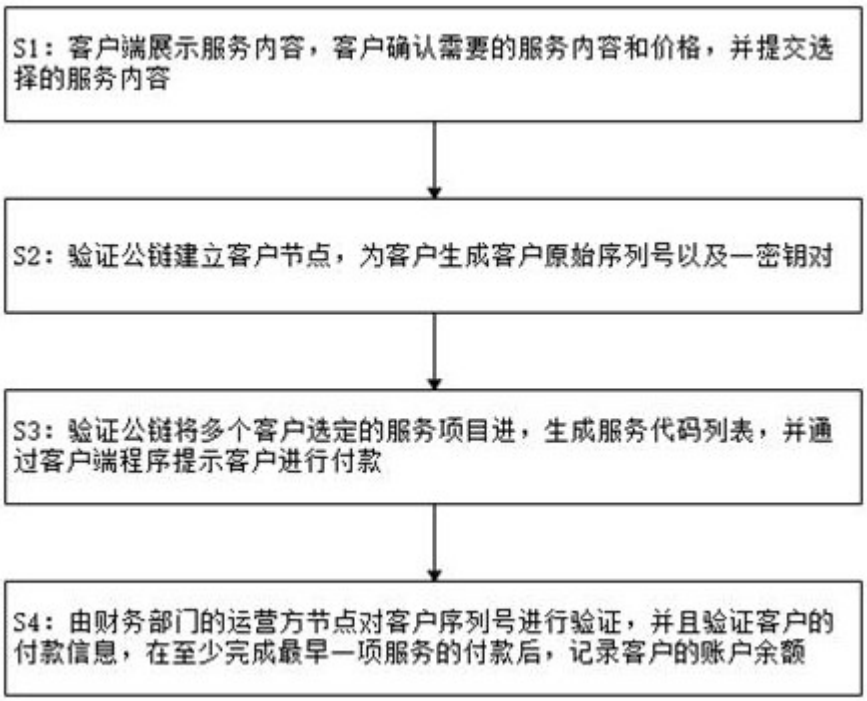

S1：客户端展示服务内容，客户确认需要的服务内容和价格，并提交选择的服务内容
S2：验证公链建立客户节点，为客户生成客户原始序列号以及一密钥对
S3：验证公链将多个客户选定的服务项目进，生成服务代码列表，并通过客户端程序提示客户进行付款
S4：由财务部门的运营方节点对客户序列号进行验证，并且验证客户的付款信息，在至少完成最早一项服务的付款后，记录客户的账户余额

图4

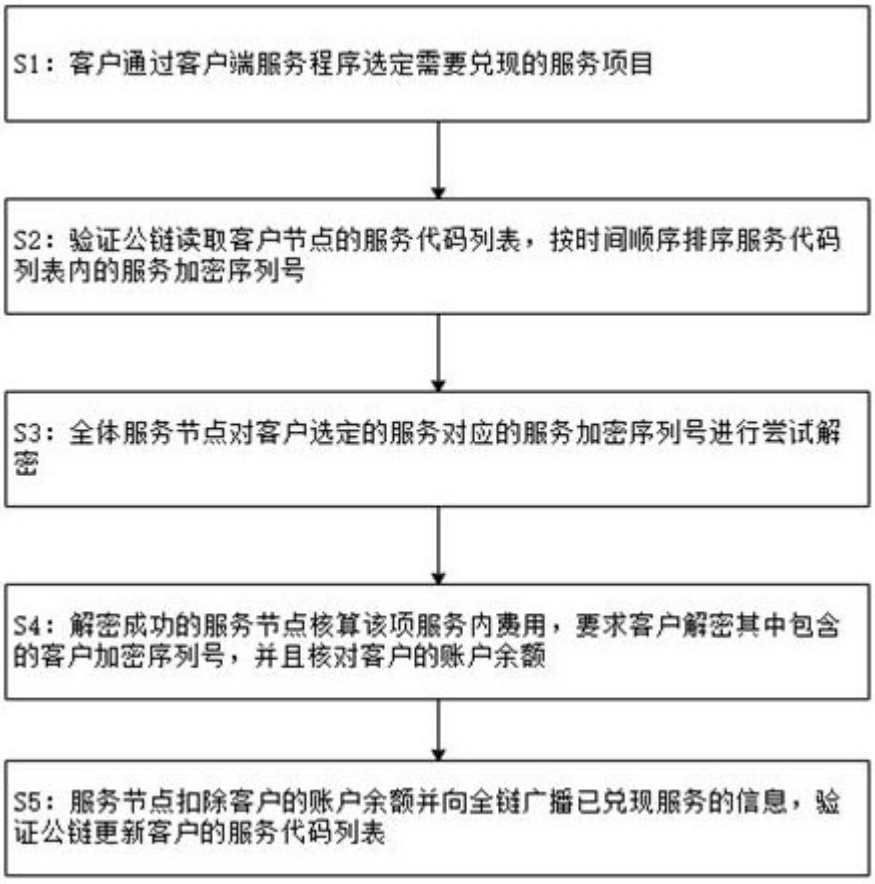

S1：客户通过客户端服务程序选定需要兑现的服务项目
S2：验证公链读取客户节点的服务代码列表，按时间顺序排序服务代码列表内的服务加密序列号
S3：全体服务节点对客户选定的服务对应的服务加密序列号进行尝试解密
S4：解密成功的服务节点核算该项服务内费用，要求客户解密其中包含的客户加密序列号，并且核对客户的账户余额
S5：服务节点扣除客户的账户余额并向全链广播已兑现服务的信息，验证公链更新客户的服务代码列表

图5