(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 109522747 A
(43)申请公布日 2019.03.26

(21)申请号 201811340635.0

(22)申请日 2018.11.12

(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201室

(72)发明人 邱炜伟 李启雷 李伟 梁秀波 尹可挺 黄方蕾

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

(51)Int.Cl.
G06F 21/62(2013.01)

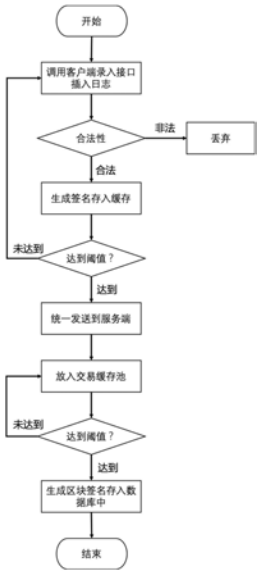
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于区块链的防篡改日志记录系统及方法

(57)摘要

本发明公开一种基于区块链的防篡改日志记录系统及方法，该系统共由录入、打包、签名、存储、审计五个模块组成相互独立的客户端和服务端，客户端拥有录入接口和定时审计接口，录入接口用于和应用系统进行对接，将需要存储的日志签名后发送到服务端；定时审计接口接收客户的审计请求，定时对服务端所存储的日志进行审计，一旦发现存在篡改痕迹，即向应用系统发起告警并阻断后续日志的录入；服务端用于验证日志签名的合法性，并将日志打包成区块，并对区块进行签名后以块链式进行存储。本发明用于企业内部的防篡改日志记录及审计等系统中，保证的日志的防篡改性，同时又提供了存储内容的可审计性，是区块链技术在中心化防篡改领域的一大突破。



CN 109522747 A

1.一种基于区块链的防篡改日志记录系统，其特征在于，所述的系统共由五个模块组成相互独立的客户端和服务端，所述的五个模块具体为：

录入模块，该模块用于检测日志的生成，将日志签名后，从客户端发送到服务端，是日志的入口模块；

打包模块，该模块对接收到的日志进行打包，并按时间生成顺序将一定量的日志打包成一个区块；

签名模块，该模块指用于对打包模块打包后的区块进行签名，采用可插拔的设计，允许多种方式的签名算法。

存储模块，该模块用于将签名后的区块以块链式进行存储，作为底层存储支撑。

审计模块，该模块用于随机审计指定时间范围内一定量的区块签名，一旦发现签名异常，客户端向其对接的应用系统推送报警；

所述的客户端拥有录入接口和定时审计接口，录入接口用于和应用系统进行对接，将需要存储的日志签名后发送到服务端；定时审计接口接收客户的审计请求，定时对服务端所存储的日志进行审计，一旦发现存在篡改痕迹，即向应用系统发起告警并阻断后续日志的录入。

所述的服务端用于验证日志签名的合法性，并将日志打包成区块，并对区块进行签名后以块链式进行存储达到防篡改目的。

2.一种基于区块链的防篡改日志记录方法，该方法基于权利要求1所述的系统实现，该方法具体包括如下步骤：

S1：所述的客户端的录入接口接收客户通过应用系统录入的日志，并检查该日志的合法性，如果合法，则客户端对其进行签名并发送到服务端，如果不合法，则拒绝该日志录入；

S2：所述的服务端调用签名模块对客户端发送的日志进行验签，并将通过合法性验证的日志暂存在日志缓存池中；

S3：所述的服务端将日志缓存池中的所有日志按时间顺序取出组成日志列表，并附上新区块编号，记为一个新的区块，然后根据日志列表的哈希、上一个区块的签名以及一个随机区块的签名三者共同为依据生成新区块的签名；其中，当新的区块为1号区块时，上一个区块的签名和随机区块的签名均为默认缺省值；当新的区块为2号区块时，上一个区块的签名和随机区块的签名均为1号区块的签名，其他区块的随机区块签名不能为其上一区块的签名；

S4：将S3签名后的区块存储到数据库中，并更新块链账本。

3.根据权利要求2所述的基于区块链的防篡改日志记录方法，所述的S1中，客户端对签名后的日志进行缓存一定量或者在规定时间窗口中不再接收到新的日志后，再将日志发送到服务端进行处理。

4.根据权利要求2所述的基于区块链的防篡改日志记录方法，所述的S3中，当服务端的日志缓存池中的日志达到一定量或者在规定时间窗口中不再接收到新的日志后，服务端对其进行打包区块的操作，已经进行排序打包的日志将会从日志缓存池中被剔除，日志缓存池进行新区块的日志缓存。

5.根据权利要求2所述的基于区块链的防篡改日志记录方法，所述的S3中，所有区块的签名及验签均使用一对公私钥对进行，所述的私钥由程序内嵌的一段随机数和程序初始化

时往数据库中存储的一段随机数共同拼接而成，并由该私钥生成公钥，然后用该私钥对区块进行签名，由该公钥对区块进行验签，保证只有服务端能对区块进行签名，服务端的部署者无法伪造签名。

一种基于区块链的防篡改日志记录系统及方法

技术领域

[0001] 本发明涉及区块链的应用领域，具体涉及一种基于区块链的防篡改日志记录系统及方法。

背景技术

[0002] 区块链是一种新型去中心化协议，能安全地存储数字货币交易或其他数据，信息不可伪造和篡改，其基本存储结构是一种按时间顺序的链式数据结构，区块链上的交易确认由区块链上的所有节点共同完成，由共识算法保证其一致性，区块链上维护一个公共的账本，公共账本位于存储区块上任何节点可见，从而保证其不可伪造和篡改。

[0003] 但是使用传统的去中心化区块链技术来应对防篡改日志方法时，去中心化的多节点冗余备份和大量日志的中心化存储理念相悖，不利于大量日志的存储和中心化的查询、审计。因此，如何利用区块链技术的同时，又能保证防篡改日志的中心化海量存储，是将区块链技术运用于防篡改日志记录的一项挑战。

发明内容

[0004] 针对现有技术的不足，本发明提出一种基于区块链的防篡改日志记录系统及方法，基于底层的区块链技术的块链式存储结构和密码学原理进行设计，保证了中心化的日志记录的防篡改性和可审计性。

[0005] 本发明的目的是通过以下技术方案来实现的：

[0006] 一种基于区块链的防篡改日志记录系统，其特征在于，所述的系统共由五个模块组成相互独立的客户端和服务端，所述的五个模块具体为：

[0007] 录入模块，该模块用于检测日志的生成，将日志签名后，从客户端发送到服务端，是日志的入口模块；

[0008] 打包模块，该模块对接收到的日志进行打包，并按时间生成顺序将一定量的日志打包成一个区块；

[0009] 签名模块，该模块指用于对打包模块打包后的区块进行签名，采用可插拔的设计，允许多种方式的签名算法；

[0010] 存储模块，该模块用于将签名后的区块以块链式进行存储，作为底层存储支撑；

[0011] 审计模块，该模块用于随机审计指定时间范围内一定量的区块签名，一旦发现签名异常，客户端向其对接的应用系统推送报警；

[0012] 所述的客户端拥有录入接口和定时审计接口，录入接口用于和应用系统进行对接，将需要存储的日志签名后发送到服务端；定时审计接口接收客户的审计请求，定时对服务端所存储的日志进行审计，一旦发现存在篡改痕迹，即向应用系统发起告警并阻断后续日志的录入；

[0013] 所述的服务端用于验证日志签名的合法性，并将日志打包成区块，并对区块进行签名后以块链式进行存储达到防篡改目的。

[0014] 一种基于区块链的防篡改日志记录方法，该方法基于上述的系统实现，该方法具体包括如下步骤：

[0015] S1：所述的客户端的录入接口接收客户通过应用系统录入的日志，并检查该日志的合法性，如果合法，则客户端对其进行签名并发送到服务端，如果不合法，则拒绝该日志录入；

[0016] S2：所述的服务端调用签名模块对客户端发送的日志进行验签，并将通过合法性验证的日志暂存在日志缓存池中；

[0017] S3：所述的服务端将日志缓存池中的所有日志按时间顺序取出组成日志列表，并附上新区块编号，记为一个新的区块，然后根据日志列表的哈希、上一个区块的签名以及一个随机区块的签名三者共同为依据生成新区块的签名；其中，当新的区块为1号区块时，上一个区块的签名和随机区块的签名均为默认缺省值；当新的区块为2号区块时，上一个区块的签名和随机区块的签名均为1号区块的签名，其他区块的随机区块签名不能为其上一区块的签名；

[0018] S4：将S3签名后的区块存储到数据库中，并更新块链账本。

[0019] 进一步地，所述的S1中，客户端对签名后的日志进行缓存一定量或者在规定时间窗口中不再接收到新的日志后，再将日志发送到服务端进行处理。

[0020] 进一步地，所述的S3中，当服务端的日志缓存池中的日志达到一定量或者在规定时间窗口中不再接收到新的日志后，服务端对其进行打包区块的操作，已经进行排序打包的日志将会从日志缓存池中被剔除，日志缓存池进行新区块的日志缓存。

[0021] 进一步地，所述的S3中，所有区块的签名及验签均使用一对公私钥对进行，所述的私钥由程序内嵌的一段随机数和程序初始化时往数据库中存储的一段随机数共同拼接而成，并由该私钥生成公钥，然后用该私钥对区块进行签名，由该公钥对区块进行验签，保证只有服务端能对区块进行签名，服务端的部署者无法伪造签名。

[0022] 本发明的有益效果如下：

[0023] 本发明中每个区块都含有区块编号、区块签名和该区块的日志列表，所有的区块按照生成的顺序进行块链式存储，每个新区块都和上一个区块以及一个随机区块有关联关系，一旦要对一条日志进行修改，首先要破解本发明的密码非对称秘钥，其次还要修改与这条日志相关的所有区块签名，这将带来很大的成本，从而达到防篡改记录日志的目的。本发明借助区块链的块链式存储结构实现中心化防篡改日志记录方法，在日志公开透明存储的情况下，即保证了日志文件仅存在增加而不能进行删除和修改，也提供了公开公信的日志防篡改审计功能。本发明的系统及方法应用于企业内部的防篡改日志记录及审计等系统中，保证的日志的防篡改性，同时又提供了存储内容的可审计性，是区块链技术在中心化防篡改领域的一大突破。

附图说明

[0024] 图1是本发明的系统中区块的内容要素图；

[0025] 图2是本发明的方法中日志底层存储的块链式组织结构图；

[0026] 图3是本发明的基于区块链的防篡改日志记录方法的流程示意图。

具体实施方式

[0027] 下面根据附图和优选实施例详细描述本发明，本发明的目的和效果将变得更加明白，以下结合附图和实施例，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仅用以解释本发明，并不用于限定本发明。

[0028] 本发明的基于区块链的防篡改日志记录系统，共由五个模块组成相互独立的客户端和服务端，五个模块具体为：

[0029] 录入模块，该模块用于检测日志的生成，将日志签名后，从客户端发送到服务端，是日志的入口模块；

[0030] 打包模块，该模块对接收到的日志进行打包，并按时间生成顺序将一定量的日志打包成一个区块；

[0031] 签名模块，该模块指用于对打包模块打包后的区块进行签名，采用可插拔的设计，允许多种方式的签名算法；

[0032] 存储模块，该模块用于将签名后的区块以块链式进行存储，作为底层存储支撑；

[0033] 审计模块，该模块用于随机审计指定时间范围内一定量的区块签名，一旦发现签名异常，客户端向其对接的应用系统推送报警；

[0034] 客户端拥有录入接口和定时审计接口，录入接口用于和应用系统进行对接，将需要存储的日志签名后发送到服务端；定时审计接口接收客户的审计请求，定时对服务端所存储的日志进行审计，一旦发现存在篡改痕迹，即向应用系统发起告警并阻断后续日志的录入；

[0035] 服务端用于验证日志签名的合法性，并将日志打包成区块，并对区块进行签名后以块链式进行存储达到防篡改目的。

[0036] 如图3所示，一种基于区块链的防篡改日志记录方法，该方法基于上述的系统实现，该方法具体包括如下步骤：

[0037] S1：所述的客户端的录入接口接收客户通过应用系统录入的日志，并检查该日志的合法性，如果合法，则客户端对其进行签名并发送到服务端，如果不合法，则拒绝该日志录入；

[0038] S2：所述的服务端调用签名模块对客户端发送的日志进行验签，并将通过合法性验证的日志暂存在日志缓存池中；

[0039] S3：所述的服务端将日志缓存池中的所有日志按时间顺序取出组成日志列表，并附上新区块编号，记为一个新的区块，然后根据日志列表的哈希、上一个区块的签名以及一个随机区块的签名三者共同为依据生成新区块的签名；其中，当新的区块为1号区块时，上一个区块的签名和随机区块的签名均为默认缺省值；当新的区块为2号区块时，上一个区块的签名和随机区块的签名均为1号区块的签名，其他区块的随机区块签名不能为其上一区块的签名(如图1-2所示)；

[0040] S4：将S3签名后的区块存储到数据库中，并更新块链账本。

[0041] 作为其中一种实施方式，所述的S1中，客户端对签名后的日志进行缓存一定量或者在规定时间窗口中不再接收到新的日志后，再将日志发送到服务端进行处理。

[0042] 作为其中一种实施方式，所述的S3中，当服务端的日志缓存池中的日志达到一定量或者在规定时间窗口中不再接收到新的日志后，服务端对其进行打包区块的操作，已经

进行排序打包的日志将会从日志缓存池中被剔除，日志缓存池进行新区块的日志缓存。

[0043] 作为其中一种实施方式，所述的S3中，所有区块的签名及验签均使用一对公私钥对进行，所述的私钥由程序内嵌的一段随机数和程序初始化时往数据库中存储的一段随机数共同拼接而成，并由该私钥生成公钥，然后用该私钥对区块进行签名，由该公钥对区块进行验签，保证只有服务端能对区块进行签名，服务端的部署者无法伪造签名。

[0044] 本发明中，每个区块都含有区块编号、区块签名和该区块的日志列表，所有的区块按照生成的顺序进行块链式存储。每个新区块都和上一个区块以及一个随机区块有关联关系，一旦要对一条日志进行修改，首先要破解本发明的密码非对称秘钥，其次还要修改与这条日志相关的所有区块签名，这将带来很大的成本，从而达到防篡改记录日志的目的。本发明借助区块链的块链式存储结构实现中心化防篡改日志记录方法，在日志公开透明存储的情况下，即保证了日志文件仅存在增加而不能进行删除和修改，也提供了公开公信的日志防篡改审计功能。

[0045] 本领域普通技术人员可以理解，以上所述仅为发明的优选实例而已，并不用于限制发明，尽管参照前述实例对发明进行了详细的说明，对于本领域的技术人员来说，其依然可以对前述各实例记载的技术方案进行修改，或者对其中部分技术特征进行等同替换。凡在发明的精神和原则之内，所做的修改、等同替换等均应包含在发明的保护范围之内。


区块
编号：No. 30
区块签名 <Signature A>
日志记录 001 <日志哈希>
日志记录 002 <日志哈希>
日志记录 010 <日志哈希>

图1

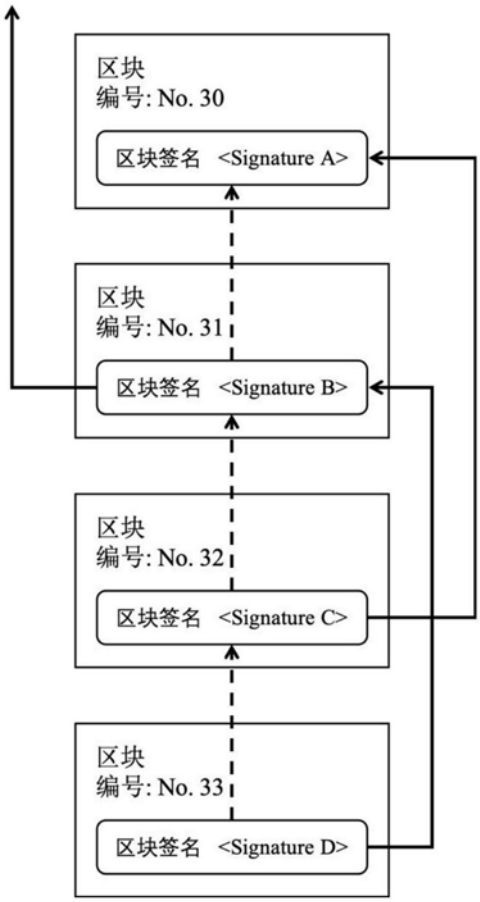

区块
编号: No. 30
区块签名 <Signature A>
区块
编号: No. 31
区块签名 <Signature B>
区块
编号: No. 32
区块签名 <Signature C>
区块
编号: No. 33
区块签名 <Signature D>

图2

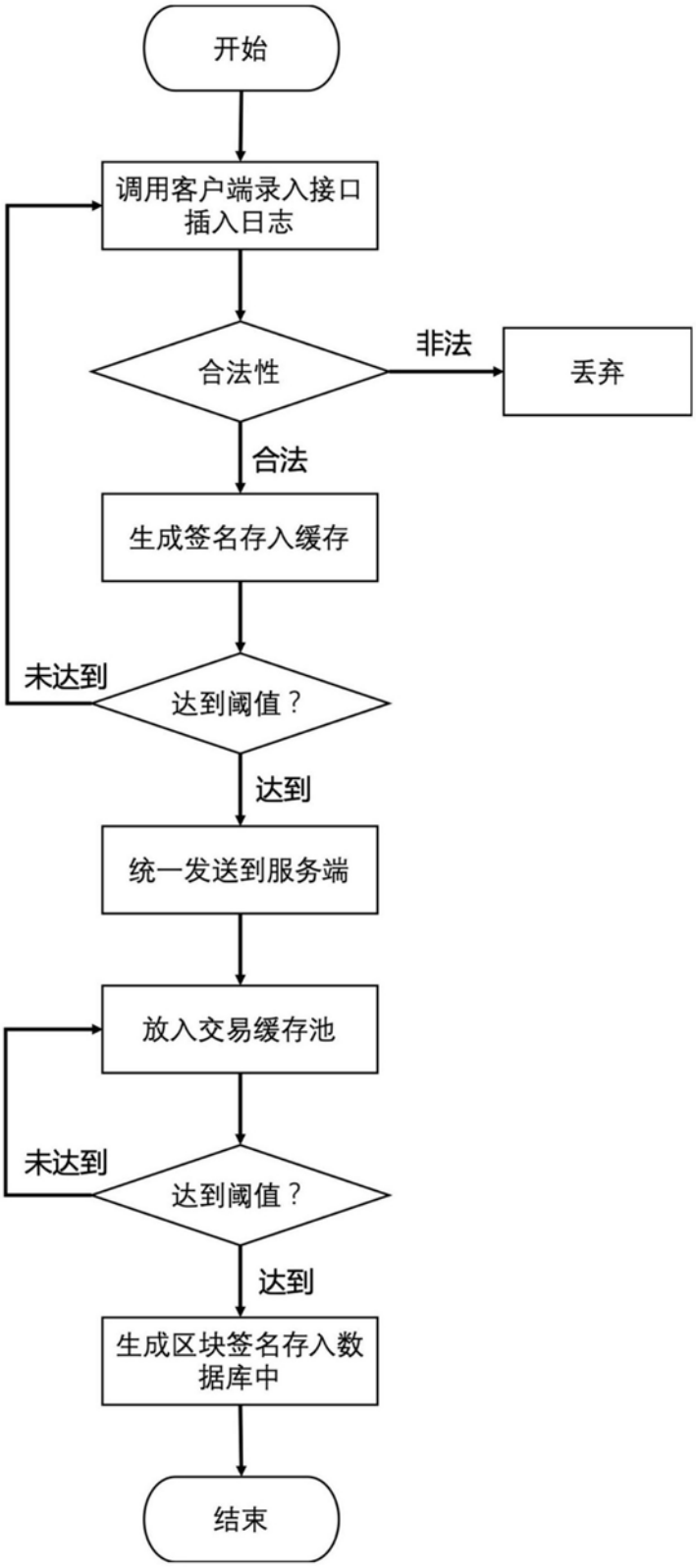

开始
调用客户端录入接口
插入日志
合法性
非法
丢弃
合法
生成签名存入缓存
未达到
达到阈值？
达到
统一发送到服务端
放入交易缓存池
未达到
达到阈值？
达到
生成区块签名存入数
据库中
结束

图3