(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 109040271 A
(43)申请公布日 2018.12.18

(21)申请号 201810927419.X

(22)申请日 2018.08.15

(71)申请人 深圳市引方科技有限公司
地址 518100 广东省深圳市龙岗区坂田天安云谷3栋B座503A

(72)发明人 邓宇平

(74)专利代理机构 北京知联天下知识产权代理事务所(普通合伙) 11594
代理人 李学康 吴鑫

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04L 9/32(2006.01)

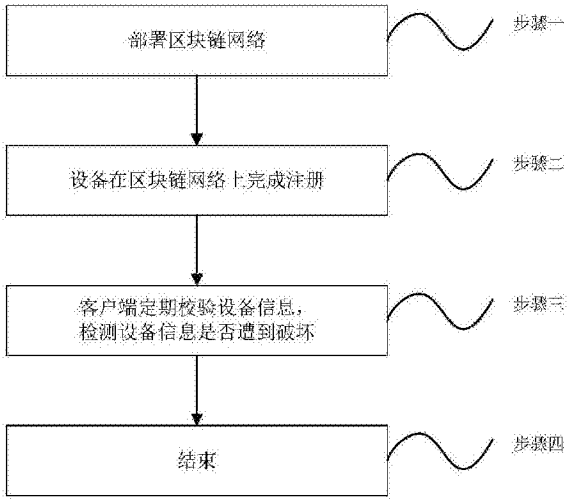
权利要求书4页 说明书10页 附图2页

(54)发明名称

一种分布式环境下的网络设备完整性保护方法

(57)摘要

针对现有基于公钥密码学身份认证的物联网设备信息完整性保护方法中,证书授权中心高度中心化、存在安全隐患的技术问题,本发明提供一种分布式环境下的网络设备完整性保护方法,包括以下步骤:第一步,基于开源项目Hyperledger Fabric部署区块链网络;第二步,物联网设备在区块链网络上进行注册;第三步,客户端定期校验设备信息,检测设备信息是否遭到破坏;第四步,结束。本发明利用区块链不可篡改性的特性,对设备信息进行永久保存,通过周期性的校验设备信息,检测设备的关键信息是否遭到篡改,从而达到保护设备信息完整性的目的,解决了去中心化带来的安全隐患。



CN 109040271 A

1.一种分布式环境下的网络设备完整性保护方法，其特征在于，包括以下步骤：

第一步，基于开源项目Hyperledger Fabric部署区块链网络，区块链网络包含C个客户端、S个提交节点和M个共识节点，C、S、M均为自然数；提交节点间相互连接，共识节点间相互连接；客户端初始化提交节点中的智能合约的时候指定背书策略，背书策略指定提交节点的一个子集用于执行背书功能，执行背书功能的提交节点又称之为背书节点；客户端部署在待保护的设备上，与背书节点、共识节点相连，客户端向背书节点发起交易提案，接收并验证背书节点返回的背书结果，并将交易提案和通过验证的背书结果发送给共识节点；每个提交节点中都维护有一条相同的区块链，存储在账本中，提交节点接收共识节点生成的区块，对区块做出验证后将其加入到区块链中，并根据仿真交易结果更新世界状态；

第二步，物联网设备在第一步部署的区块链网络上进行注册；

第三步，客户端定期校验设备信息，检测设备信息是否遭到破坏；

第四步，结束。

2.如权利要求1所述的分布式环境下的网络设备完整性保护方法，其特征在于，所述第一步部署的区块链网络中，客户端中除了安装有软件开发包，还安装有保密存储单元、ID生成模块、信息读取模块和哈希值计算模块；软件开发包读取设备保密单元存储的设备信息，生成交易提案并向背书节点的智能合约发送交易提案，接收背书节点的智能合约发送的仿真交易结果和背书签名，验证仿真交易结果和背书策略并将交易提案和仿真交易结果发送给共识节点中的共识服务；保密存储单元用于接收并存储ID生成模块和哈希值计算模块发送的信息，保密单元存储的信息用于软件开发包的读取；ID生成模块生成设备ID，并将设备ID发送至保密存储单元；信息读取模块读取设备配置信息，并将设备信息发送至哈希值计算模块；哈希值计算模块接收配置信息读取模块发送的设备配置信息，并计算设备信息哈希值，然后将设备信息哈希值发送至保密存储单元；

提交节点中包含有账本、背书模块、提交模块和智能合约；所有的提交节点中都会维护一个相同的账本，账本中包括区块链和世界状态；区块链是一系列按照时间顺序、通过哈希值连在一起成链状的区块，用来记录历史交易；世界状态是一个键值数据库，世界状态的数据存储模型可根据业务逻辑进行自定义，世界状态中存储了区块链网络中每一个账户的状态信息，世界状态随着区块链中交易的执行进行更新；背书模块接收客户端发起的交易提案，进行仿真交易，将仿真交易结果发送给发起交易提案的客户端；提交模块接收共识节点生成的区块，对区块做出验证后将区块加入区块链中；智能合约本质上是管理区块链网络中的不同实体间相互作用或交易的业务逻辑，客户端通过调用智能合约可以设置和查询账本；智能合约接收客户端发送的交易提案，读取账本中的世界状态，根据世界状态仿真执行交易，并将仿真交易结果发送给背书模块；智能合约中除了安装有调用模块，查询模块和写入模块，还安装有信息注册模块和信息校验模块；调用模块接收信息注册交易提案，并根据交易提案类型将信息注册交易提案发送给信息注册模块，接收信息校验交易提案，并根据交易提案类型将信息校验交易提案发送给信息校验模块；信息校验模块通过查询模块查询世界状态中是否存在信息校验交易提案中的设备ID，查询模块读取世界状态中的设备注册因子，并发送给信息校验模块，信息校验模块对比信息校验交易提案中的注册因子和世界状态中的注册因子，得到信息校验结果；信息注册模块从调用模块接收信息注册交易提案，通过查询模块获取当前账本中的世界状态，信息注册模块调用写入模块，写入模块对设备

信息注册因子按照账本中世界状态的数据格式进行打包，生成将要写入世界状态的写操作数据集合，并将写操作数据集合返回给信息注册模块；

共识节点上包含有共识服务模块；共识服务模块接收客户端发送的交易提案和背书结果，采用共识算法对T时间段内的交易提案进行排序，并将这些交易提案打包成区块广播至所有提交节点的提交模块，时间段T的大小根据用户需求设置；此外，共识服务也会对仿真交易结果做出验证后广播至所有提交模块。

3.如权利要求1所述的分布式环境下的网络设备完整性保护方法，其特征在于，所述第二步物联网设备在第一步部署的区块链网络上进行注册，包括以下步骤：

2.1客户端向背书节点发送信息注册交易提案；

2.2背书节点的智能合约仿真执行信息注册交易提案，为智能合约执行结果进行签名，并将智能合约执行结果、背书节点签名作为信息注册交易提案结果返回给客户端；

2.3客户端检验背书策略指定的背书节点集合中所有背书节点发来的仿真交易结果，若智能合约执行结果一致，客户端将信息注册交易提案和智能合约执行结果广播给区块链网络中所有的共识节点；否则，返回错误信息，转第四步；

2.4共识节点生成区块，验证智能合约执行结果，并将新生成的区块和通过验证的智能合约执行结果广播给区块链网络中所有的提交节点；对于未通过验证的智能合约执行结果，返回错误结果，转第四步；

2.5提交节点更新账本，方法是：提交模块将新生成的区块加入区块链中，并根据智能合约执行结果更新世界状态。

4.如权利要求1所述的分布式环境下的网络设备完整性保护方法，其特征在于，所述第三步，客户端定期校验设备信息，检测设备信息是否遭到破坏，具体流程如下：

3.1客户端生成设备的信息注册因子，根据信息注册因子和请求类型生成信息校验交易提案，然后向所有背书策略指定的背书节点的智能合约发送信息校验交易提案；

3.2背书节点的智能合约仿真执行信息校验交易提案，得到信息校验结果和背书节点的签名，若世界状态中存在该设备ID，将信息校验结果和背书节点的签名作为信息校验提案结果返回给客户端；若不存在，则显示错误信息，转第四步；

3.3客户端对信息校验交易提案结果做出解析，校验交易提案结果的签名，并将信息校验交易提案广播给区块链网络中所有的共识节点；

3.4共识节点对于接收到的注册交易提案按照时间顺序进行记录，将注册交易提案按照区块的数据结构生成区块，并将新生成的区块广播给区块链网络中所有的提交节点；

3.5提交节点的提交模块将新区块加入区块链中。

5.如权利要求3所述的分布式环境下的网络设备完整性保护方法，其特征在于，所述步骤2.1客户端向背书节点发送信息注册交易提案，包括以下步骤：

2.1.1客户端的ID生成模块为物联网设备生成ID，并将设备ID发送至保密存储单元；

2.1.2客户端的信息读取模块读取设备信息；设备信息是指物联网设备的固件信息和配置信息，这些信息可通过相应的API获得；

2.1.3信息读取模块将设备固件信息和配置信息发送给哈希值计算模块；

2.1.4哈希值计算模块计算设备固件信息哈希值和配置信息哈希值，并将设备固件信息哈希值和配置信息哈希值发送至保密存储单元；

2.1.5软件开发包读取保密存储单元中的信息，并生成信息注册因子，信息注册因子包括设备ID、设备固件信息哈希值和配置信息哈希值；

2.1.6软件开发包根据注册因子和请求类型生成信息注册交易提案；交易提案是一个调用智能合约的请求，用来确认哪些数据可以读取或写入账本；

2.1.7客户端的软件开发包向所有背书策略指定的背书节点发送信息注册交易提案。

6.如权利要求3所述的分布式环境下的网络设备完整性保护方法，其特征在于，所述步骤2.2具体流程如下：

2.2.1智能合约的调用模块接收信息注册交易提案，并根据交易提案类型将信息注册交易提案发送给信息注册模块；

2.2.2信息注册模块通过查询模块获取当前账本中的世界状态，若世界状态中已存在该设备ID，则返回错误信息，转第四步，否则转步骤2.2.3；

2.2.3信息注册模块调用写入模块，写入模块对设备信息注册因子按照账本中世界状态的数据格式进行打包，生成将要写入世界状态的写操作数据集合，并将写操作数据集合返回给信息注册模块；此写操作数据集合即为智能合约执行结果；

2.2.4背书模块为智能合约执行结果进行签名；

2.2.5背书节点将智能合约执行结果、背书节点签名作为信息注册交易提案结果返回给客户端的软件开发包。

7.如权利要求3所述的分布式环境下的网络设备完整性保护方法，其特征在于，所述步骤2.3具体流程如下：

2.3.1客户端软件开发包验证背书节点签名，确定信息注册交易提案结果是否来自背书策略指定的背书节点集合，若符合背书策略，转步骤2.3.2，否则显示错误信息，转第四步；

2.3.2客户端对比各背书节点生成的智能合约执行结果，若智能合约执行结果一致，转步骤2.3.3，否则返回错误信息，转第四步；

2.3.3客户端将信息注册交易提案和智能合约执行结果广播给区块链网络中所有的共识节点。

8.如权利要求3所述的分布式环境下的网络设备完整性保护方法，其特征在于，所述步骤2.4具体流程如下：

2.4.1共识服务模块对接收到的所有的信息注册交易提案按照时间顺序进行记录；

2.4.2共识节点将注册交易提案按照区块的数据结构生成区块；

2.4.3共识节点验证智能合约执行结果是否正确，若正确，转步骤2.4.4，否则，返回错误结果，转第四步；

2.4.4共识节点新生成的区块和通过验证的智能合约执行结果广播给区块链网络中所有的提交节点。

9.如权利要求4所述的分布式环境下的网络设备完整性保护方法，其特征在于，所述步骤3.2包括以下步骤：

3.2.1智能合约中的调用模块接收信息校验交易提案，并根据交易提案类型将信息校验交易提案发送给信息校验模块；

3.2.2信息校验模块通过查询模块查询世界状态中是否存在信息校验交易提案中的设

备ID,若世界状态中存在该设备ID,则执行步骤3.2.3,若不存在,则显示错误信息,转第四步;

3.2.3查询模块读取世界状态中的设备注册因子,并发送给信息校验模块;

3.2.4信息校验模块对比信息校验交易提案中的注册因子和世界状态中的注册因子,得到信息校验结果;

3.2.5背书模块对信息校验结果进行签名;

3.2.6背书节点将信息校验结果和背书节点的签名作为信息校验提案结果返回给客户端的软件开发包。

一种分布式环境下的网络设备完整性保护方法

技术领域

[0001] 本发明涉及计算机网络技术领域，特别涉及物联网中一种分布式环境下的网络设备完整性保护方法。

背景技术

[0002] 通常情况下，数据的完整性依赖于对系统中心或第三方实体的信任，如系统的主节点、中心数据库，以及系统的负责人、数据库的管理员等，一旦上述系统中心不再可信(例如管理员被收买或数据库遭入侵)，将会破坏数据的完整性，且很难被发现。

[0003] 现有的物联网设备信息完整性保护方法基于公钥基础设施(PKI，Public Key Infrastructure)，它利用公钥密码学的特点，通过第三方可信机构，即证书授权中心(CA，Certificate Authority)，建立一套证书发放、管理和使用的体系，来支持和完成网络系统中的身份认证、信息加密，从而保证数据完整性和抗抵赖性。

[0004] 现有的物联网设备信息完整性保护方法基于公钥密码学的身份认证，方法是：

[0005] 第一步，设备向证书授权中心请求秘钥分发。

[0006] 第二步，证书授权中心生成公钥和私钥。

[0007] 第三步，证书授权中心将公钥分发给设备，同时将私钥分发给设备的授权管理对象。

[0008] 第四步，设备通过签名机制辨别授权的设备信息更改请求，方法是：

[0009] 4.1设备接收设备信息更改请求。

[0010] 4.2设备使用公钥验证设备信息更改请求是否经由设备授权管理对象用私钥进行加密(即签名)。

[0011] 4.3若设备信息更改请求经由设备授权管理对象签名，则接收设备信息更改请求；若设备请求未经设备授权管理对象签名或经由非设备授权管理对象签名，则拒绝设备信息更改请求。

[0012] 现有的物联网设备信息完整性保护方法基于公钥密码学的身份认证，其中高度中心化的证书授权中心会产生以下几个问题：第一，在通信过程中产生任何问题、证书授权中心无法做出相应的解决对策时，通信双方将无法解决这个问题，导致最后问题的不了了之；第二，证书授权中心一旦遭受攻击，整个物联网系统将会受到很大的损害，严重者导致整个物联网系统瘫痪；第三，若攻击者对通信过程的信息进行篡改，则通信的双方无法获知信息已被篡改。

[0013] 区块链最初是由一位化名为中本聪的人为比特币(一种数字货币)而设计出的一种特殊的分布式记账技术。比特币以及由其衍生出来的区块链技术都引入了签名系统、共识机制、时间戳等技术，各模块之间的相互协作完美地解决了去中心化带来的安全隐患。因此，区块链并不是一项全新的互联网技术，而是多项已有技术，如非对称密钥签名、共识机制、时间戳、哈希算法、P2P通信等的巧妙整合。区块链技术基于去中心化的对等网络，把密码学原理、时序数据和共识机制相结合，来保障分布式数据库中各节点的连贯和持续，使信

息能即时验证、可追溯、但难以篡改和无法屏蔽，从而创造了一套隐私、高效、安全的共享价值体系。

[0014] 从数据角度来看，区块链是由包含交易信息的区块按照生成区块的时间有序链接起来的数据结构，它能够使参与者对全网交易记录的事件顺序和当前状态建立共识。如图1所示，区块链网络的每个区块包含它的前一区块哈希值，这样把每个区块链接到各自前一区块的哈希值序列就创建了一条一直可以追溯到第一个区块(创世块)的链条。

[0015] 区块链的每个区块由区块头和存储内容组成。区块头包含6个数据域，分别为：区块ID、前一区块哈希值、时间戳、根哈希值、目标值、随机数。区块中的存储内容分别为：区块大小、交易计数、交易信息。区块ID是对每一个区块的编号，用于验证区块和交易完成后查看交易信息；前一区块哈希值是指与当前区块相连的上一个区块的根哈希值，创世区块的前一区块根哈希值为0；时间戳记录了当前区块生成的时间；根哈希值是将交易信息里面的各条交易信息通过计算哈希树合并而成；目标值规定了用户争夺当前区块记账权难度系数；随机数是当前区块工作量证明的参数，通过不断调整随机数的值来改变当前区块头的哈希值，计算出小于等于目标值的区块头哈希值的用户节点获得该区块的记账权，并获得相应的奖励。区块大小记录了当前区块所占内存大小；交易计数记录了当前区块中记录的交易数量；交易信息记录了当前区块保存的所有交易细节。

[0016] 在比特币的基础上，以太坊项目进一步扩展了区块链网络的能力，从交易延伸为智能合约。与比特币系统相比，以太坊做出了多方面的改进，比如减少了平均出块时间、压缩了区块大小、货币不限量、加入了叔伯块激励、哈希树由一棵增加为了三棵。

[0017] 以太坊最主要的特点是增加了智能合约和账户系统。智能合约区块链系统中的应用，是已编码的、可自动运行的业务逻辑，通常有自己的代币和专用开发语言。账户是比特币中没有涉及的，由于比特币的匿名性，系统中无需加入账户的设计。以太坊通过借助账户来确定价值归属，所有以太坊区块链上的状态转换都是账户之间价值和信息的转移。账户分为外部账户和合约账户，外部账户由用户通过私钥控制，合约账户则是由智能合约来控制。作为一个平台运行智能合约的去中心化平台，平台上的应用按程序设定运行，不存在停机、审查、欺诈、第三方人为干预的可能。以太坊提供了一条公开的区块链，并制定了面向智能合约的一套编程语言，智能合约开发者可以在其上使用官方提供的工具来开发支持以太坊区块链协议的应用。

[0018] Hyperledger(超级账本)是一个透明、公开、去中心化的分布式账本项目，由Linux基金会牵头，联合包括IBM和思科在内的30家初始企业创立。Hyperledger首次提出和实现完备的权限管理、创新的一致性算法和可插拔、可扩展的框架。如果说以比特币为代表的货币型区块链技术为1.0，以以太坊为代表的智能合约型区块链技术为2.0，那么实现了完备的权限控制和安全保障的Hyperledger项目毫无疑问代表着区块链3.0时代的到来。

[0019] 超级账本架构(Hyperledger Fabric)是Hyperledger中的一个区块链项目，项目全称为Architecture of the Hyperledger Blockchain Fabric。与其他区块链技术类似，Hyperledger Fabric是一个包含一个账本，使用智能合约并且是一个通过所有参与者管理交易的系统。Hyperledger Fabric与其他区块链系统最大的不同体现在私有和许可，通过成员管理实现了完备的权限控制和安全保障。

[0020] Hyperledger Fabric的账本包含两个组件：世界状态和区块链。在Hyperledger

Fabric网络中的每一个参与者都拥有一个账本的副本。世界状态组件描述了账本在特定时间点的状态，它是账本的数据库。区块链记录了产生世界状态当前值的所有交易，它是世界状态的更新历史。

[0021] 当一个区块链外部的一个应用程序需要访问账本时，就会调用智能合约。大多数情况下，智能合约只会查询账本的数据库组件——世界状态，但不会查询交易记录。

[0022] Hyperledger Fabric提供了多个可拔插选项。账本数据可被存储为多种格式，共识机制可被接入或者断开，同时支持多种不同的成员管理模式。

[0023] Hyperledger Fabric提供了建立通道的功能，这允许参与者为交易新建一个单独的账本。当网络中的一些参与者是竞争对手时，这个功能变得尤为重要。因为这些参与者并不希望所有的交易信息——比如提供给部分客户的特定价格信息——都对网络中所有参与者公开。只有在同一个通道中的参与者，才会拥有该通道中的账本，而其他不在此通道中的参与者则看不到这个账本。

[0024] 在区块链网络中，不同的参与者写入的交易必须按照产生顺序依次被写入账本中。要实现这一目标，必须正确的建立交易顺序并且必须包含拒绝错误(或者恶意)插入账本中的无效交易的方法，这就是区块链中的共识机制。Hyperledger Fabric被设计为允许网络构建者依据业务需求来选择采用的共识机制。

[0025] 区块链技术中的共识机制在去中心化的思想上解决了节点间互相信任的问题，保证了区块链如何在分布式场景下达成一致性。当前具有代表性的共识算法有工作量证明(PoW，Proof of Work)、股权证明(PoS，Proof of Stake)、实用拜占庭容错算法(PBFT，Practical Byzantine Fault Tolerance)。以比特币为代表的货币型区块链大都采用工作量证明共识算法，主要用于争夺区块的记账权。区块链网络中上的客户端基于算力来争夺记账权，从而获得比特币收益，这一操作被称为挖矿。基于工作量证明的区块链网络实现了完全去中心化，网络中的节点可以做到自由进出，破坏系统花费的成本巨大。但是，工作量证明共识算法对节点的性能和网络环境要求高，并且造成了很大的资源浪费。以比特股、量子链等为代表的智能合约型区块链采用股权证明共识算法，该算法提出，区块链上的记录和证明应该由那些在链上具有经济利益的人来维护和保障。通过要求证明人提供一定数量的数字货币所有权而非进行难度极高的工作量证明，股权证明算法从根本上摆脱了工作量证明算法的能源浪费问题，但还是需要挖矿，没有在本质上解决商业应用的痛点。实用拜占庭容错算法是在拜占庭将军问题场景下产生的一种基于消息传递的共识算法。异步网络环境下实用拜占庭容错算法所能允许的最大容错数为(n-1)/3，n为总节点数。超级账本目前采用实用拜占庭容错算法，该算法需经过预准备、准备、执行三个阶段达成一致性，而这三阶段任何一阶段出错都会导致整个共识过程失败。

[0026] 区块链技术的出现为设备关键信息完整性保护提供了可行的方案。区块链作为一种分布式存储技术，能够有效避免对中心节点的依赖，各节点通过共识机制达到存储数据的一致性，即便有部分节点遭受攻击，其他节点存储的数据也可以支撑整个系统继续运行。另外，存储在区块链中的数据具有不可篡改的特性，即便节点被入侵或者攻击者来自系统内部，也无法篡改区块链中的数据。数据一旦存入区块链的数据块中将无法删除、修改，只能新增，保障了数据的长效性；区块链记录着每个交易，且交易数据不可被篡改，保障了数据的可溯源性；在结构中的任何节点都能对数据的完整性进行验证。在校验文件的完整性

时，只需要将待校验文件的特征值与原文件的特征值对比，如果相同，说明文件没有发生改动，否则说明文件被篡改。

[0027] 通过查阅资料发现，目前没有公开文献涉及将区块链用于设备信息完整性保护的方法。

发明内容

[0028] 针对现有基于公钥密码学身份认证的物联网设备信息完整性保护方法中，证书授权中心高度中心化、存在安全隐患的技术问题，本发明提供一种分布式环境下的网络设备完整性保护方法，利用区块链不可篡改性的特性，对设备信息进行永久保存，通过周期性的校验设备信息，检测设备的关键信息是否遭到篡改，从而达到保护设备信息完整性的目的。

[0029] 本发明的技术方案如下：

[0030] 第一步，基于开源项目Hyperledger Fabric部署区块链网络，区块链网络包含C个客户端、S个提交节点和M个共识节点，C、S、M均为自然数；提交节点间相互连接，共识节点间相互连接；客户端初始化提交节点中的智能合约的时候指定背书策略，背书策略指定提交节点的一个子集用于执行背书功能，执行背书功能的提交节点又称之为背书节点；客户端部署在待保护的设备上，与背书节点、共识节点相连，客户端向背书节点发起交易提案，接收并验证背书节点返回的背书结果，并将交易提案和通过验证的背书结果发送给共识节点；每个提交节点中都维护有一条相同的区块链，存储在账本中，提交节点接收共识节点生成的区块，对区块做出验证后将其加入到区块链中，并根据仿真交易结果更新世界状态；

[0031] 第二步，物联网设备在第一步部署的区块链网络上进行注册；

[0032] 第三步，客户端定期校验设备信息，检测设备信息是否遭到破坏；

[0033] 第四步，结束。

[0034] 1.作为本发明技术方案的进一步改进，所述第一步部署的区块链网络中，客户端中除了安装有软件开发包，还安装有保密存储单元、ID生成模块、信息读取模块和哈希值计算模块；软件开发包读取设备保密单元存储的设备信息，生成交易提案并向背书节点的智能合约发送交易提案，接收背书节点的智能合约发送的仿真交易结果和背书签名，验证仿真交易结果和背书策略并将交易提案和仿真交易结果发送给共识节点中的共识服务；保密存储单元用于接收并存储ID生成模块和哈希值计算模块发送的信息，保密单元存储的信息用于软件开发包的读取；ID生成模块生成设备ID，并将设备ID发送至保密存储单元；信息读取模块读取设备配置信息，并将设备信息发送至哈希值计算模块；哈希值计算模块接收配置信息读取模块发送的设备配置信息，并计算设备信息哈希值，然后将设备信息哈希值发送至保密存储单元；

[0035] 提交节点中包含有账本、背书模块、提交模块和智能合约；所有的提交节点中都会维护一个相同的账本，账本中包括区块链和世界状态；区块链是一系列按照时间顺序、通过哈希值连在一起成链状的区块，用来记录历史交易；世界状态是一个键值数据库，世界状态的数据存储模型可根据业务逻辑进行自定义，世界状态中存储了区块链网络中每一个账户的状态信息，世界状态随着区块链中交易的执行进行更新；背书模块接收客户端发起的交易提案，进行仿真交易，将仿真交易结果发送给发起交易提案的客户端；提交模块接收共识节点生成的区块，对区块做出验证后将区块加入区块链中；智能合约本质上是管理区块链

网络中的不同实体间相互作用或交易的业务逻辑，客户端通过调用智能合约可以设置和查询账本；智能合约接收客户端发送的交易提案，读取账本中的世界状态，根据世界状态仿真执行交易，并将仿真交易结果发送给背书模块；智能合约中除了安装有调用模块，查询模块和写入模块，还安装有信息注册模块和信息校验模块；调用模块接收信息注册交易提案，并根据交易提案类型将信息注册交易提案发送给信息注册模块，接收信息校验交易提案，并根据交易提案类型将信息校验交易提案发送给信息校验模块；信息校验模块通过查询模块查询世界状态中是否存在信息校验交易提案中的设备ID，查询模块读取世界状态中的设备注册因子，并发送给信息校验模块，信息校验模块对比信息校验交易提案中的注册因子和世界状态中的注册因子，得到信息校验结果；信息注册模块从调用模块接收信息注册交易提案，通过查询模块获取当前账本中的世界状态，信息注册模块调用写入模块，写入模块对设备信息注册因子按照账本中世界状态的数据格式进行打包，生成将要写入世界状态的写操作数据集合，并将写操作数据集合返回给信息注册模块；

[0036] 共识节点上包含有共识服务模块；共识服务模块接收客户端发送的交易提案和背书结果，采用共识算法对T时间段内的交易提案进行排序，并将这些交易提案打包成区块广播至所有提交节点的提交模块，时间段T的大小根据用户需求设置；此外，共识服务也会对仿真交易结果做出验证后广播至所有提交模块。

[0037] 1.作为本发明技术方案的进一步改进，所述第二步物联网设备在第一步部署的区块链网络上进行注册，包括以下步骤：

[0038] 2.1客户端向背书节点发送信息注册交易提案；

[0039] 2.2背书节点的智能合约仿真执行信息注册交易提案，为智能合约执行结果进行签名，并将智能合约执行结果、背书节点签名作为信息注册交易提案结果返回给客户端；

[0040] 2.3客户端检验背书策略指定的背书节点集合中所有背书节点发来的仿真交易结果，若智能合约执行结果一致，客户端将信息注册交易提案和智能合约执行结果广播给区块链网络中所有的共识节点；否则，返回错误信息，转第四步；

[0041] 2.4共识节点生成区块，验证智能合约执行结果，并将新生成的区块和通过验证的智能合约执行结果广播给区块链网络中所有的提交节点；对于未通过验证的智能合约执行结果，返回错误结果，转第四步；

[0042] 2.5提交节点更新账本，方法是：提交模块将新生成的区块加入区块链中，并根据智能合约执行结果更新世界状态。

[0043] 作为本发明技术方案的进一步改进，所述第三步，客户端定期校验设备信息，检测设备信息是否遭到破坏，具体流程如下：

[0044] 3.1客户端生成设备的信息注册因子，根据信息注册因子和请求类型生成信息校验交易提案，然后向所有背书策略指定的背书节点的智能合约发送信息校验交易提案；

[0045] 3.2背书节点的智能合约仿真执行信息校验交易提案，得到信息校验结果和背书节点的签名，若世界状态中存在该设备ID，将信息校验结果和背书节点的签名作为信息校验提案结果返回给客户端；若不存在，则显示错误信息，转第四步；

[0046] 3.3客户端对信息校验交易提案结果做出解析，校验交易提案结果的签名，并将信息校验交易提案广播给区块链网络中所有的共识节点；

[0047] 3.4共识节点对于接收到的注册交易提案按照时间顺序进行记录，将注册交易提

案按照区块的数据结构生成区块，并将新生成的区块广播给区块链网络中所有的提交节点；

[0048] 3.5提交节点的提交模块将新区块加入区块链中。

[0049] 作为本发明技术方案的进一步改进，所述步骤2.1客户端向背书节点发送信息注册交易提案，包括以下步骤：

[0050] 2.1.1客户端的ID生成模块为物联网设备生成ID，并将设备ID发送至保密存储单元。

[0051] 2.1.2客户端的信息读取模块读取设备信息。设备信息是指物联网设备的固件信息和配置信息，这些信息可通过相应的API获得。

[0052] 2.1.3信息读取模块将设备固件信息和配置信息发送给哈希值计算模块。

[0053] 2.1.4哈希值计算模块通过md5算法计算设备固件信息哈希值和配置信息哈希值，并将设备固件信息哈希值和配置信息哈希值发送至保密存储单元。

[0054] 2.1.5软件开发包读取保密存储单元中的信息，并生成信息注册因子，信息注册因子包括设备ID、设备固件信息哈希值和配置信息哈希值。

[0055] 2.1.6软件开发包根据注册因子和请求类型生成信息注册交易提案。交易提案是一个调用智能合约的请求，用来确认哪些数据可以读取或写入账本。

[0056] 2.1.7客户端的软件开发包向所有背书策略指定的背书节点发送信息注册交易提案。

[0057] 1.作为本发明技术方案的进一步改进，所述步骤2.2具体流程如下：

[0058] 2.2.1智能合约的调用模块接收信息注册交易提案，并根据交易提案类型将信息注册交易提案发送给信息注册模块；

[0059] 2.2.2信息注册模块通过查询模块获取当前账本中的世界状态，若世界状态中已存在该设备ID，则返回错误信息，转第四步，否则转步骤2.2.3；

[0060] 2.2.3信息注册模块调用写入模块，写入模块对设备信息注册因子按照账本中世界状态的数据格式进行打包，生成将要写入世界状态的写操作数据集合，并将写操作数据集合返回给信息注册模块；此写操作数据集合即为智能合约执行结果；

[0061] 2.2.4背书模块为智能合约执行结果进行签名；

[0062] 2.2.5背书节点将智能合约执行结果、背书节点签名作为信息注册交易提案结果返回给客户端的软件开发包。

[0063] 作为本发明技术方案的进一步改进，所述步骤2.3具体流程如下：

[0064] 2.3.1客户端软件开发包验证背书节点签名，确定信息注册交易提案结果是否来自背书策略指定的背书节点集合，若符合背书策略，转步骤2.3.2，否则显示错误信息，转第四步；

[0065] 2.3.2客户端对比各背书节点生成的智能合约执行结果，若智能合约执行结果一致，转步骤2.3.3，否则返回错误信息，转第四步；

[0066] 2.3.3客户端将信息注册交易提案和智能合约执行结果广播给区块链网络中所有的共识节点。

[0067] 作为本发明技术方案的进一步改进，所述步骤2.4具体流程如下：

[0068] 2.4.1共识服务模块对接收到的所有的信息注册交易提案按照时间顺序进行记

录。

[0069] 2.4.2共识节点将注册交易提案按照区块的数据结构生成区块。

[0070] 2.4.3共识节点验证智能合约执行结果是否正确，若正确，转步骤2.4.4，否则，返回错误结果，转第四步。

[0071] 2.4.4共识节点新生成的区块和通过验证的智能合约执行结果广播给区块链网络中所有的提交节点。

[0072] 作为本发明技术方案的进一步改进，所述步骤3.2包括以下步骤：

[0073] 3.2.1智能合约中的调用模块接收信息校验交易提案，并根据交易提案类型将信息校验交易提案发送给信息校验模块。

[0074] 3.2.2信息校验模块通过查询模块查询世界状态中是否存在信息校验交易提案中的设备ID，若世界状态中存在该设备ID，则执行步骤3.2.3，若不存在，则显示错误信息，转第四步。

[0075] 3.2.3查询模块读取世界状态中的设备注册因子，并发送给信息校验模块。

[0076] 3.2.4信息校验模块对比信息校验交易提案中的注册因子和世界状态中的注册因子，得到信息校验结果。

[0077] 3.2.5背书模块对信息校验结果进行签名。

[0078] 3.2.6背书节点将信息校验结果和背书节点的签名作为信息校验提案结果返回给客户端的软件开发包。

[0079] 本发明可以获得以下技术效果：

[0080] 本发明利用区块链不可篡改性的特性，对设备信息进行永久保存，通过周期性的校验设备信息，检测设备的关键信息是否遭到篡改，从而达到保护设备信息完整性的目的，解决了去中心化带来的安全隐患。

附图说明

[0081] 图1是背景技术和本发明区块链结构图。

[0082] 图2是本发明总体流程图。

[0083] 图3是本发明第一步构建的区块链网络逻辑结构图。

[0084] 图4是本发明第一步区块链网络的软件结构示意图。

具体实施方式

[0085] 以下将结合说明书附图和具体实施例对本发明做进一步详细说明。

[0086] 如图2所示，本发明一种分布式环境下的网络设备完整性保护方法，包括以下步骤：

[0087] 第一步，基于开源项目Hyperledger Fabric部署区块链网络，区块链网络包括客户端、提交节点和共识节点。其中在客户端初始化提交节点中的智能合约的时候会指定背书策略，背书策略指定了提交节点的一个子集用于执行背书功能，执行背书功能的提交节点又称之为背书节点。如图3所示，所述区块链网络包含多个客户端、多个提交节点和多个共识节点，提交节点间相互连接，共识节点间相互连接。其中，无箭头的线表示节点间通过网络连接，有箭头的线表示信息的输入输出。客户端部署在待保护的设备上，客户端与背书

节点、共识节点相连，客户端向背书节点发起交易提案，接收并验证背书节点返回的背书结果，并将交易提案和通过验证的背书结果发送给共识节点。每个提交节点中都维护有一条相同的区块链，存储在账本中，提交节点接收共识节点生成的区块，对区块做出验证后将其加入到区块链中，并根据仿真交易结果更新世界状态。

[0088] 如图4所示，客户端中除了安装有软件开发包，还安装有保密存储单元、ID生成模块、信息读取模块和哈希值计算模块。软件开发包读取设备保密单元存储的设备信息，生成交易提案并向背书节点的智能合约发送交易提案，接收背书节点的背书模块发送的仿真交易结果和背书签名，验证仿真交易结果和背书策略并将交易提案和仿真交易结果发送给共识节点中的共识服务。保密存储单元用于接收并存储ID生成模块、信息读取模块和哈希值计算模块发送的信息，保密单元存储的信息用于软件开发包的读取。ID生成模块生成设备ID，并将设备ID发送至保密存储单元。信息读取模块读取设备配置信息，并将设备信息发送至哈希值计算模块。哈希值计算模块接收配置信息读取模块发送的设备配置信息，并计算设备信息哈希值，然后将设备信息哈希值发送至保密存储单元。

[0089] 如图4所示，提交节点中包含有账本、背书模块、提交模块和智能合约。所有的提交节点中都会维护一个相同的账本，账本中包括区块链和世界状态。区块链是一系列按照时间顺序、通过哈希值连在一起成链状的区块，用来记录历史交易。世界状态是一个键值数据库，世界状态的数据存储模型可根据业务逻辑进行自定义，世界状态中存储了区块链网络中每一个账户的状态信息，世界状态随着区块链中交易的执行进行更新。背书模块接收客户端发起的交易提案，进行仿真交易，将仿真交易结果发送给发起交易提案的客户端。提交模块接收共识节点生成的区块，对区块做出验证后将区块加入区块链中。智能合约本质上是管理区块链网络中的不同实体间相互作用或交易的业务逻辑，客户端通过调用智能合约可以设置和查询账本。智能合约接收客户端发送的交易提案，读取账本中的世界状态，根据世界状态仿真执行交易，并将仿真交易结果发送给背书模块。智能合约中除了安装有调用模块，查询模块和写入模块，还安装有信息注册模块和信息校验模块。

[0090] 如图4所示，共识节点上包含有共识服务模块。共识服务模块接收客户端发送的交易提案和背书结果，采用共识算法对一段时间内的交易提案进行排序，并将这些交易提案打包成区块广播至所有提交节点的提交模块。此外，共识服务也会对仿真交易结果做出验证后广播至所有提交模块。

[0091] 在基于Hyperledger Fabric的区块链网络中，客户端向所有背书策略指定的背书节点发送交易提案。背书节点利用部署在其中的智能合约执行提案并将生成的提案结果返回给客户端，客户端收到足够多的提案结果后，验证背书节点签名，并比较各背书节点返回的提案结果，判断提案结果是否一致以及是否参照指定的背书策略执行。然后将交易提案和提案结果以消息形式广播给共识节点。共识节点根据其共识算法生成交易账本，并把结果广播给所有的提交节点。

[0092] 第二步，物联网设备在第一步部署的区块链网络上进行注册。方法是：

[0093] 2.1客户端向背书节点发送信息注册交易提案，方法是：

[0094] 2.1.1客户端的ID生成模块为物联网设备生成ID，并将设备ID发送至保密存储单元。

[0095] 2.1.2客户端的信息读取模块读取设备信息。设备信息是指物联网设备的固件信

息和配置信息，这些信息可通过相应的API获得。

[0096] 2.1.3信息读取模块将设备固件信息和配置信息发送给哈希值计算模块。

[0097] 2.1.4哈希值计算模块通过md5算法计算设备固件信息哈希值和配置信息哈希值，并将设备固件信息哈希值和配置信息哈希值发送至保密存储单元。

[0098] 2.1.5软件开发包读取保密存储单元中的信息，并生成信息注册因子，信息注册因子包括设备ID、设备固件信息哈希值和配置信息哈希值。

[0099] 2.1.6软件开发包根据注册因子和请求类型生成信息注册交易提案。交易提案是一个调用智能合约的请求，用来确认哪些数据可以读取或写入账本。

[0100] 2.1.7客户端的软件开发包向所有背书策略指定的背书节点发送信息注册交易提案。

[0101] 2.2背书节点的智能合约仿真执行信息注册交易提案并与客户端交互，方法是：

[0102] 2.2.1智能合约的调用模块接收信息注册交易提案，并根据交易提案类型将信息注册交易提案发送给信息注册模块。

[0103] 2.2.2信息注册模块通过查询模块获取当前账本中的世界状态，若世界状态中已存在该设备ID，则返回错误信息，转第四步，否则转步骤2.2.3。

[0104] 2.2.3信息注册模块调用写入模块，写入模块对设备信息注册因子按照账本中世界状态的数据格式进行打包，生成将要写入世界状态的写操作数据集合，并将写操作数据集合返回给注册模块。此写操作数据集合即为智能合约执行结果。

[0105] 2.2.4背书模块为智能合约执行结果进行签名。

[0106] 2.2.5背书节点将智能合约执行结果、背书节点签名作为信息注册交易提案结果返回给客户端的软件开发包。

[0107] 2.3客户端检验背书策略指定的背书节点集合中所有背书节点发来的仿真交易结果并与共识节点交互，方法是：

[0108] 2.3.1客户端软件开发包验证背书节点签名，确定信息注册交易提案结果是否来自背书策略指定的背书节点集合，若符合背书策略，转步骤2.3.2，否则显示错误信息，转第四步。

[0109] 2.3.2客户端对比各背书节点生成的智能合约执行结果，若智能合约执行结果一致，转步骤2.3.3，否则返回错误信息，转第四步。

[0110] 2.3.3客户端将信息注册交易提案和智能合约执行结果广播给区块链网络中所有的共识节点。

[0111] 2.4共识节点生成区块并与提交节点交互，方法是：

[0112] 2.4.1共识服务模块对接收到的所有的信息注册交易提案按照时间顺序进行记录。

[0113] 2.4.2共识节点将注册交易提案按照区块的数据结构生成区块。

[0114] 2.4.3共识节点验证智能合约执行结果是否正确，若正确，转步骤2.4.4，否则，返回错误结果，转第四步。

[0115] 2.4.4共识节点新生成的区块和通过验证的智能合约执行结果广播给区块链网络中所有的提交节点。

[0116] 2.5提交节点更新账本，方法是：

[0117] 2.5.1提交模块将新生成的区块加入区块链中。

[0118] 2.5.2提交模块根据智能合约执行结果更新世界状态。

[0119] 第三步，客户端定期校验设备信息，检测设备信息是否遭到破坏。

[0120] 3.1客户端向背书节点发送信息校验交易提案，方法是：

[0121] 3.1.1软件开发包执行步骤2.1.1至2.1.5，重新生成设备的信息注册因子。

[0122] 3.1.2软件开发包根据信息注册因子和请求类型生成信息校验交易提案。

[0123] 3.1.3软件开发包向所有背书策略指定的背书节点的智能合约发送信息校验交易提案。

[0124] 3.2背书节点的智能合约仿真执行信息校验交易提案并与客户端交互，方法是：

[0125] 3.2.1智能合约中的调用模块接收信息校验交易提案，并根据交易提案类型将信息校验交易提案发送给信息校验模块。

[0126] 3.2.2信息校验模块通过查询模块查询世界状态中是否存在信息校验交易提案中的设备ID，若世界状态中存在该设备ID，则执行步骤3.2.3，若不存在，则显示错误信息，转第四步。

[0127] 3.2.3查询模块读取世界状态中的设备注册因子，并发送给信息校验模块。

[0128] 3.2.4信息校验模块对比信息校验交易提案中的注册因子和世界状态中的注册因子，得到信息校验结果。

[0129] 3.2.5背书模块对信息校验结果进行签名。

[0130] 3.2.6背书节点将信息校验结果和背书节点的签名作为信息校验提案结果返回给客户端的软件开发包。

[0131] 3.3客户端对信息校验交易提案结果做出解析并与共识节点交互，方法是：

[0132] 3.3.1软件开发包验证信息校验交易提案结果的签名，若信息校验提案结果来自于合法的背书节点，转步骤3.3.2，否则返回错误信息，转第四步。

[0133] 3.2.2若信息校验交易提案结果中的信息对比结果相同，说明设备信息未经篡改，否则说明信息被篡改。

[0134] 3.3.3客户端将信息校验交易提案广播给区块链网络中所有的共识节点。

[0135] 3.4共识节点生成区块并与提交节点交互，方法是：

[0136] 3.4.1共识节点对于接收到的注册交易提案按照时间顺序进行记录。

[0137] 3.4.2共识节点将注册交易提案按照区块的数据结构生成区块。

[0138] 3.4.4共识节点将新生成的区块广播给区块链网络中所有的提交节点。

[0139] 3.5提交节点的提交模块将新区块加入区块链中。

[0140] 第四步，结束。

[0141] 以上仅是本发明的优选实施方式，本发明的保护范围并不仅局限于上述实施例，凡属于本发明思路下的技术方案均属于本发明的保护范围。应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理前提下的若干改进和润饰，应视为本发明的保护范围。

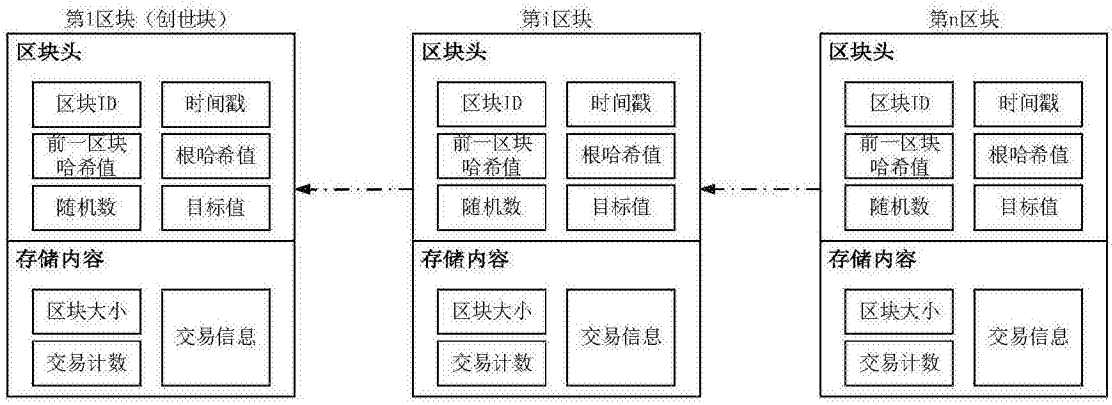

第1区块（创世块）
区块头
区块ID
时间戳
前一区块哈希值
根哈希值
随机数
目标值
存储内容
区块大小
交易计数
交易信息
第i区块
区块头
区块ID
时间戳
前一区块哈希值
根哈希值
随机数
目标值
存储内容
区块大小
交易计数
交易信息
第n区块
区块头
区块ID
时间戳
前一区块哈希值
根哈希值
随机数
目标值
存储内容
区块大小
交易计数
交易信息

图1

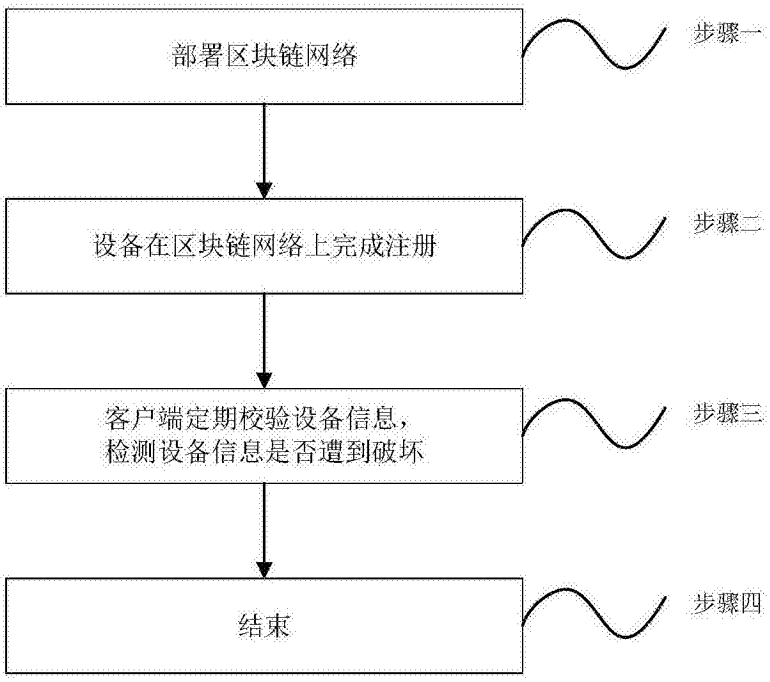

部署区块链网络
步骤一
设备在区块链网络上完成注册
步骤二
客户端定期校验设备信息，
检测设备信息是否遭到破坏
步骤三
结束
步骤四

图2

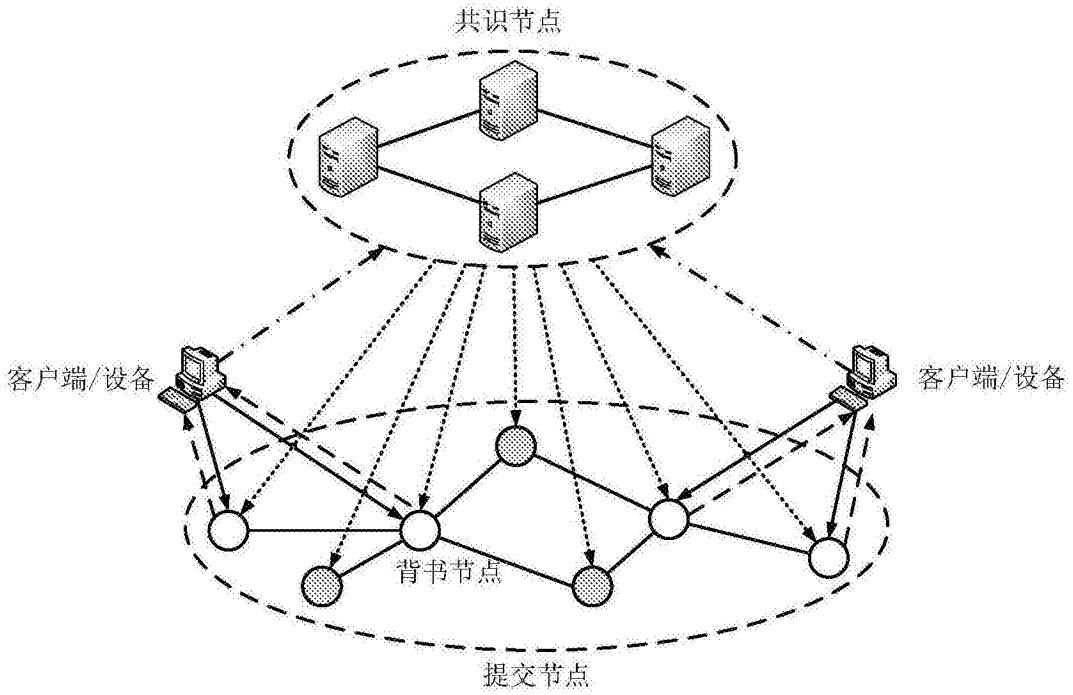

共识节点
客户端/设备
客户端/设备
背书节点
提交节点

图3

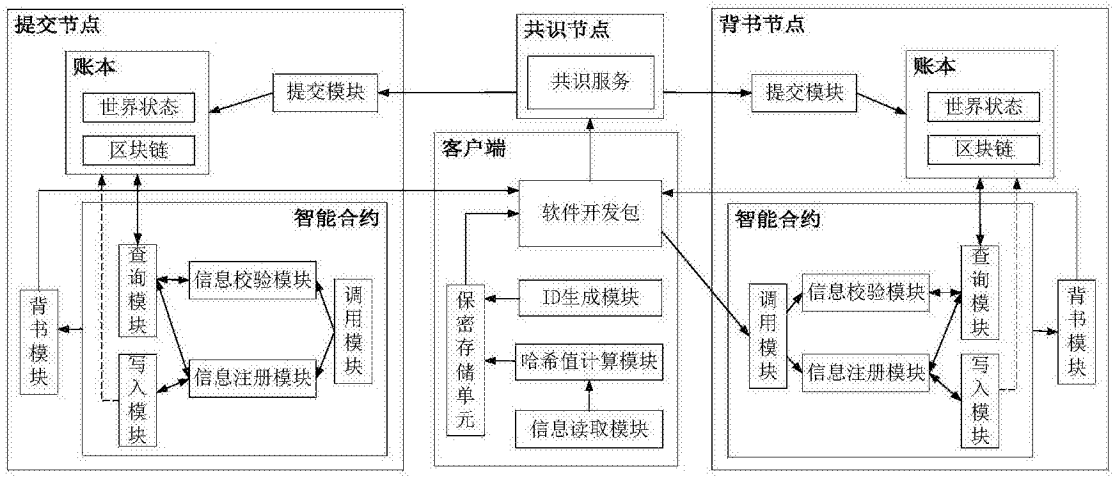

提交节点
账本
世界状态
区块链
提交模块
智能合约
查询模块
信息校验模块
调用模块
背书模块
写入模块
信息注册模块
共识节点
共识服务
客户端
软件开发包
保密存储单元
ID生成模块
哈希值计算模块
信息读取模块
背书节点
提交模块
账本
世界状态
区块链
智能合约
调用模块
信息校验模块
查询模块
背书模块
信息注册模块
写入模块

图4