基于区块链CPOW共识算法的智能合约网关

申请号：201710610316.6
申请日：2017-07-25

申请(专利权)人 光载无限(北京)科技有限公司
地址 100036 北京市海淀区西八里庄北里56号院1号写字楼五层
发明(设计)人 焦继佩

主分类号 H04L29/08(2006.01)I
分类号 H04L29/08(2006.01)I H04L29/06(2006.01)I G06Q20/38(2012.01)I G06Q20/06(2012.01)I G06Q20/02(2012.01)I
公开(公告)号 107360238A
公开(公告)日 2017-11-17
专利代理机构
代理人

(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 107360238 A
(43)申请公布日 2017.11.17

(21)申请号 201710610316.6

(22)申请日 2017.07.25

(71)申请人 光载无限(北京)科技有限公司
地址 100036 北京市海淀区西八里庄北里56号院1号写字楼五层

(72)发明人 焦继佩

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
G06Q 20/38(2012.01)
G06Q 20/06(2012.01)
G06Q 20/02(2012.01)

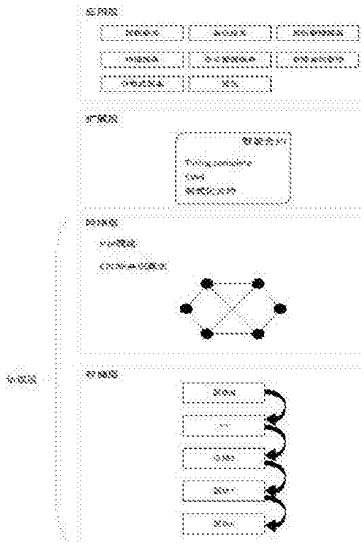
权利要求书2页 说明书7页 附图2页

(54)发明名称

基于区块链CPOW共识算法的智能合约网关

(57)摘要

本发明是一种基于区块链CPOW共识算法的智能合约网关,包括协议层、扩展层和应用层,协议层包括网络层和存储层,网络层包括p2p网络和CPOW共识算法,存储层将数据信息存储在区块链上;扩展层基于比特币协定与原系统的可程式化交易脚本,提供与以太坊虚拟机兼容的协定方式定义的基本交易种类;应用层包含与智能合约网关相关的各项服务,帮助用户快速上手区块链服务。本发明为第三方开发者提供基于区块链的强大支持,兼容更多的应用,让区块链更快的应用到客户端中;本发明提出的CPOW算法,不仅解决了51%攻击的问题,而且大幅度提升了交易的性能,使基于区块链CPOW共识算法的智能合约网关上建立应用的成本和速度都大大改善。



CN 107360238 A

1.一种基于区块链CPOW共识算法的智能合约网关，其特征在于，所述智能合约网关包括协议层、扩展层和应用层，其中，

所述协议层包括相互独立但不可以分割的网络层和存储层，所述网络层包括p2p网络和CPOW共识算法；

所述存储层将数据信息存储在区块链上；

所述扩展层基于比特币协定与原系统的可程式化交易脚本，提供与以太坊虚拟机兼容的协定方式定义的基本交易种类，与系统提供的进阶程式化交易脚本配合，达到原比特币无法完成的智能合约；

所述应用层包含与智能合约网关相关的各项服务，应用层提供的服务使用者可根据需求自行选择以上各项服务，帮助用户快速上手区块链服务。

2.根据权利要求1所述的智能合约网关，其特征在于，所述协议层的工作机制如下：

(1)当通过网络层传入过来的数据时，发送节点将新的数据记录向全网进行广播；

(2)接收节点对收到的数据记录信息进行检验，检验记录信息是否合法，通过验证后数据记录将被纳入到一个区块中；

(3)全网所有接收节点对区块执行CPOW共识算法；

(4)区块通过共识算法过程后被正式纳入区块链中存储，全网节点均表示接受该区块，而表示接受的方法，就是该区块的随机散列值视为最新的区块散列值，该区块的制造将以该区块链为基础进行延长。

3.根据权利要求2所述的智能合约网关，其特征在于，所述应用层包含的各项服务为：

(1)授权服务和鉴证服务：使用本网关固有的登录授权服务，授权成功则返回一个openid区分不同的用户：

(2)身份管理服务：管理用户的身份信息；

(3)特征服务：存储相关数据信息；

(4)签名管理服务：数据传输过程中提供签名处理；

(5)智能合约管理服务：可以自定义合约，也可以对现有合约进行处理。

4.根据权利要求3所述的智能合约网关，其特征在于，所述基于区块链CPOW共识算法的智能合约网关通过图灵完备的脚本执行，透过EVM协定方式，提供制定化合约，藉由API和区块链进行沟通，智能合约的内容和行为记录在区块链上。

5.根据权利要求4所述的智能合约网关，其特征在于，所述CPOW共识算法是在比特币POW的基础上采用动态非线性工作量证明机制，调整每个矿工获选为验证者的困难度，避免趋向独占验证的可能性，解决了51%攻击的问题，而且缩短了平均区块的确认时间。

6.根据权利要求5所述的智能合约网关，其特征在于，所述CPOW共识算法的逻辑过程如下：

(1)打包交易，检索待确认交易内存池，选择包含进区块的交易；

(2)构造Coinbase，确定了包含进区块的交易集后，就可以统计本区块手续费总额，结合产出规则，矿工可以计算自己本区块的收益；

(3)构造hashMerkleRoot，对所有交易构造Merkle数；

(4)填充其他字段，获得完整区块头；

(5)CPOW运算，在动态非线性工作量证明机制中，根据当时的时间点往回推算N-1个区

块，每一个参与的矿工依照此N-1个区块中获选位验证者的次数，对区块头进行CPOW运算；

动态调整其在当时挖矿的困难度，也就是调整工作量证明的期望值大小；

(6)验证结果，如果符合难度，则广播到全网，挖下一个块；不符合难度则根据一定策略改变以上某个字段后再进行CPOW运算并验证。

基于区块链CPOW共识算法的智能合约网关

技术领域

[0001] 本发明涉及计算机应用程序，尤其是涉及基于区块链CPOW共识算法的智能合约网关，为第三方开发者提供基于区块链的强大支持，让区块链更快的应用到客户端中。

背景技术

[0002] 比特币是一种P2P形式的数字货币，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性，从技术上来说比特币是点对点数字货币系统，整个系统是基于UTXO的交易模型建立的，侧重点是在交易和数据结构的布局及记录。在算哈希和工作量证明上，比特币是基于矿工计算唯一正确的哈希值，来证明工作量来获得记账打包区块权，从而获得奖励，这个用的就是工作量证明(Pow)。

[0003] 以太坊是点对点的去中心化的虚拟机，是一款能够在区块链上实现智能合约、开源的底层系统。从技术上来说以太坊是虚拟机，完整的说法应该是智能合约虚拟机，也就是侧重按照合约的模式执行合约的虚拟机。所以，以太坊是基于Account模型的(也有地方说EVM，就智能合约虚拟机，为什么说Account，是账户模式，以太坊是基于账户体系的)。以太坊虽然在比特币基础学习了一些，但也创造了新的模式，为后面开发者提供了思路，同时，后面开发应用者基本是在这两种模式下选择一种作为自己的应用模式。在算哈希和工作量证明上，以太坊希望优化比特币这方面的工作，因为比特币挖矿的这种模式算力比较集中，比如专业的矿机出现，第二页比较浪费电力，浪费社会资源。提出权益证明机制(Pos)，能避免一定的算力集中和资源浪费。

[0004] 区块链(Blockchain)是在没有中央控制点的分布式对等网络，使用分布式集体运作的方法，实现一套不可篡改的，可信任的数据库技术方案，其特点为去中心化存储、信息高度透明、不易篡改等。再通俗一点说，区块链就是利用计算机程序在全网记录所有交易信息的“公开大账本”。区块链网络中的节点，通过计算一个艰难的计算问题，来获得记账的权利；任何区块链网络上的节点，都可以观察到整个总账；区块链数据由每个节点共同维护，每个参与维护节点都能复制获得一份完整数据库的拷贝，除非能够同时控制整个系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容。比特币和以太坊都是成功的区块链技术应用，是最典型的代表。再细说点，有了比特币才有区块链技术，有了以太坊人们才认识到区块链还可以独立出来，不仅仅是比特币才能有区块链技术，也是以太坊为后面开启了区块链世界的思路思想。因为都是区块链技术的应用，所以底层基础思路是一样的。都是点对点的网络节点、公开的账本、共识基础算法，都是通过挖矿来维护网络。

[0005] 比特币生态和以太坊生态两种区块链存在兼容性问题，尽管比特币和以太坊的运

营都是以分布式分类账和加密技术的原则为基础，两者仍旧在众多技术领域存在不同如下：

从技术上来说比特币是点对点数字货币系统，整个系统是基于UTXO的交易模型建立的，侧重点是在交易和数据结构的布局及记录。在算哈希和工作量证明上，比特币是基于矿工计算唯一正确的哈希值，来证明工作量来获得记账打包区块权，从而获得奖励，这个用的就是工作量证明(Pow)。在基本算法上比特币使用的是安全散列算法，SHA-256。

[0006] 从技术上来说，以太坊是虚拟机，完整的说法应该是智能合约虚拟机，也就是侧重按照合约的模式执行合约的虚拟机。所以呢以太坊是基于Account模型的(也有地方说EVM，就智能合约虚拟机，为什么说Account，是账户模式，以太坊是基于账户体系的)。所以呢，以太坊虽然在比特币基础学习了一些，但也创造了新的模式，为后面开发者提供了思路，同时呢后面开发应用者基本是在这两种模式下选择一种作为自己的应用模式。在算哈希和工作量证明上，以太坊希望优化比特币这这方面的工作，因为比特币挖矿的这种模式算力比较集中，比如专业的矿机出现，第二页比较浪费电力，浪费社会资源。提出权益证明机制(Pos)，能避免一定的算力集中和资源浪费。在基本算法上以太坊使用的是ethash。

[0007] 从语言上来说：以太坊使用的编程语言是Turning complete，而比特币使用的则是基于栈的编程语言。

[0008] 所以在实际运用过程中如果想把比特币，以太坊融合并兼容到应用里面存在相当大的困难，耗时耗力。

[0009] 比特币和以太坊两种区块链的51%攻击问题：比特币以及目前大部分加密货币都采用了POW即工作量证明的机制来实现共识，通过计算来猜测一个数值(nonce)，得以解决规定的 hash 问题。保证在一段时间内，系统中只能出现少数合法结果。同时，这些少量的合法结果会在网络中进行广播，收到的用户进行验证后会基于它认为的最长链上继续难题的计算。因此，系统中可能出现链的分叉(Fork)，但最终会有一条链成为最长的链。hash问题具有不可逆的特点，因此，目前除了暴力计算外，还没有有效的算法进行解决。反之，如果获得符合要求的nonce，则说明在概率上是付出了对应的算力。谁的算力多，谁最先解决问题的概率就越大。当掌握超过全网一半算力时，从概率上就能控制网络中链的走向。这也是所谓51%攻击的由来。如果有人掌握了50%以上的算力，他能够比其他人更快地找到开采区块需要的那个随机数，因此他实际上拥有了绝对哪个一区块的有效权利。使他能够1、修改自己的交易记录，这可以使他进行双重支付；2、阻止区块确认部分或者全部交易；3、阻止部分或全部矿工开采到任何有效的区块。

发明内容

[0010] 本发明的目的是针对比特币生态和以太坊生态的兼容性问题，提出基于区块链CPOW共识算法的智能合约网关，该平台使开发人员能够建立和发布下一代分布式应用，平台上面提供各种模块让用户来搭建应用，改善建立应用的成本和速度，解决51%攻击的问题，大幅度提升了交易的性能。

[0011] 为了实现本发明的目的，采用以下技术方案：

一种基于区块链CPOW共识算法的智能合约网关，所述智能合约网关包括协议层、扩展层和应用层，其中，

所述协议层包括相互独立但不可以分割的网络层和存储层，所述网络层包括p2p网络和CPOW共识算法。所述存储层将数据信息存储在区块链上；

所述扩展层基于比特币协定与原系统的可程式化交易脚本，提供与以太坊虚拟机兼容的协定方式定义的基本交易种类，与系统提供的进阶程式化交易脚本配合，达到原比特币无法完成的智能合约；

所述应用层包含与智能合约网关相关的各项服务，应用层提供的服务使用者可根据需求自行选择以上各项服务，帮助用户快速上手区块链服务。

[0012] 所述协议层的工作机制如下：

(1)当通过网络层传入过来的数据时，发送节点将新的数据记录向全网进行广播；

(2)接收节点对收到的数据记录信息进行检验，检验记录信息是否合法，通过验证后数据记录将被纳入到一个区块中；

(3)全网所有接收节点对区块执行CPOW共识算法；

(4)区块通过共识算法过程后被正式纳入区块链中存储，全网节点均表示接受该区块，而表示接受的方法，就是该区块的随机散列值视为最新的区块散列值，该区块的制造将以该区块链为基础进行延长。

[0013] 所述应用层包含的各项服务为：

(1)授权服务和鉴证服务：使用本网关固有的登录授权服务，授权成功则返回一个openid区分不同的用户：

(2)身份管理服务：管理用户的身份信息；

(3)特征服务：存储相关数据信息；

(4)签名管理服务：数据传输过程中提供签名处理；

(5)智能合约管理服务：可以自定义合约，也可以对现有合约进行处理。

[0014] 所述基于区块链CPOW共识算法的智能合约网关通过图灵完备的脚本执行，透过EVM协定方式，提供制定化合约，藉由API和区块链进行沟通，智能合约的内容和行为记录在区块链上。

[0015] 所述CPOW共识算法是在比特币POW的基础上采用动态非线性工作量证明机制，调整每个矿工获选为验证者的困难度，避免趋向独占验证的可能性，解决了51%攻击的问题，而且缩短了平均区块的确认时间。

[0016] 所述CPOW共识算法的逻辑过程如下：

(1)打包交易，检索待确认交易内存池，选择包含进区块的交易；

(2)构造Coinbase，确定了包含进区块的交易集后，就可以统计本区块手续费总额，结合产出规则，矿工可以计算自己本区块的收益；

(3)构造hashMerkleRoot，对所有交易构造Merkle数；

(4)填充其他字段，获得完整区块头；

(5)CPOW运算，在动态非线性工作量证明机制中，根据当时的时间点往回推算N-1个区块，每一个参与的矿工依照此N-1个区块中获选位验证者的次数，对区块头进行CPOW运算。动态调整其在当时挖矿的困难度，也就是调整工作量证明的期望值大小；

(6)验证结果，如果符合难度，则广播到全网，挖下一个块；不符合难度则根据一定策略改变以上某个字段后再进行CPOW运算并验证。

[0017] 本发明从区块链的协议层出发，把开发目标指向应用层，为第三方开发者提供基于区块链的强大支持，兼容更多的应用，让区块链更快的应用到客户端中；

本发明提出的CPOW算法，通过调整每个矿工获选为验证者的困难度，避免趋向独占验证的可能性，不仅解决了51%攻击的问题，而且大幅度提升了交易的性能。

[0018] 如果将搭建应用比作造房子，那么基于区块链CPOW共识算法的智能合约网关就提供了墙面、屋顶、地板等模块，用户只需像搭积木一样把房子搭起来，使基于区块链CPOW共识算法的智能合约网关上建立应用的成本和速度都大大改善。

附图说明

[0019] 图1是基于区块链CPOW共识算法的智能合约网关底层架构；

图2是智能合约网关协议层的工作机制。

具体实施方式

[0020] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合附图和具体实施例，对本发明进一步详细说明。

[0021] 图1是基于区块链CPOW共识算法的智能合约网关底层架构；从架构设计上来说，基于区块链CPOW共识算法的智能合约网关可以简单的分为三个层次，协议层、扩展层和应用层。其中，

1、协议层包括网络层和存储层，它们相互独立但不可以分割，存储层主要是把一些数据信息存储在区块链上，网络层包括p2p网络和CPOW共识算法。协议层的工作机制如下：

(1)当通过网络层传入过来的数据时，发送节点会将新的数据记录向全网进行广播；

(2)接收节点对收到的数据记录信息进行检验，比如记录信息是否合法，通过验证后数据记录将被纳入到一个区块中，

(3)全网所有接收节点对区块执行CPOW共识算法

(4)区块通过共识算法过程后被正式纳入区块链中存储，全网节点均表示接受该区块，而表示接受的方法，就是该区块的随机散列值视为最新的区块散列值，该区块的制造将以该区块链为基础进行延长。

[0022] 2、扩展层也称为智能合约层，该智能合约功能是基于比特币协定与原有之可程式化的交易脚本，虽然比特币可以提供可程式化的交易脚本，但是功能较为局限，无法涵盖各种需求，而且不支持较复杂的计算。比特币倾向支持比较简单的交易脚本。一些比较特殊的脚本并不保证会被比特币部分网络节点接受。该智能合约层提供可以与以太坊虚拟机兼容的协定方式定义的基本交易种类。配上系统提供的进阶程式化交易脚本，可以达到原比特币无法完成的智能合约，例如提供自动执行的功能，此即为比特币无法运行的计算。与此同时，此层也提供制式化合约，通过该网关提供的API可以与其沟通，用户不须具备专编程背景也能快速来建构属于自己的合约。基于比特币之上，该智能合约层的交易脚本可以打造图灵完备。图灵完备使该网关成为可解决通用问题的一种方案。由于区块链需多数节点来验证交易是否通过，使得该网关可成为一种具备公信力的通用解决方案而适合应用在各公开方案以及私有联盟上。

[0023] 3、应用层包含授权服务、鉴证服务，身份管理服务，特征服务，签名管理服务，智能

合约管理服务等，帮助用户快速上手区块链服务。应用层提供的服务使用者可根据需求自行选择以下服务：

(1)授权服务和鉴证服务：可以使用本网关固有的登录授权服务，如果授权成功则返回一个openid区分不同的用户；

(2)身份管理服务：主要管理用户的身份信息；

(3)特征服务：主要存储一些数据信息；

(4)签名管理服务：数据传输过程中提供签名处理；

(5)智能合约管理服务：可以自定义合约，也可以对现有合约进行处理。

[0024] 基于区块链CPOW共识算法的智能合约网关主要通过Turing complete(图灵完备)的脚本执行，透过EVM(Ethereum Virtual Machine)协定方式，提供制定化合约，藉由API和区块链进行沟通，智能合约的内容和行为记录在区块链上，有利于自动化的合约履行，因为合约、数据都完全放在区块链上，履行合约可完全在区块链上完成，不须外部介入，以最有效率的方式执行合约。图灵完备使基于区块链CPOW共识算法的智能合约网关成为可解决通用问题的一种方案。该平台可以实现和比特币生态和以太坊生态的兼容性，并通过移动端的战略，促进区块链技术的产品化和提高区块链行业的易用性，旨在将真实商业社会与区块链世界连接。使更多应用相应的兼容。

[0025] 针对比特币和以太坊的51%攻击问题，我们提出了CPOW共识算法。CPOW共识算法是在比特币POW的基础上采用动态非线性工作量证明机制，调整每个矿工获选为验证者的困难度，避免趋向独占验证的可能性，解决了51%攻击的问题。而且缩短了平均区块的确认时间，目标区块创建时间为15s，而比特币的平均区块创建时间是10分钟，大幅度提升了每秒交易的性能，相当于原本比特币每秒交易的40倍。

[0026] 其逻辑过程如下：

(1)打包交易，检索待确认交易内存池，选择包含进区块的交易。矿工可以任意选择，甚至可以不选择(挖空块)，因为每一个区块有容量限制(当前是1M)，所以矿工也不能无限选择。对于矿工来说，最合理的策略是首先根据手续费对待确认交易集进行排序，然后由高到低尽量纳入最多的交易。

[0027] (2)构造Coinbase，确定了包含进区块的交易集后，就可以统计本区块手续费总额，结合产出规则，矿工可以计算自己本区块的收益。

[0028] (3)构造hashMerkleRoot，对所有交易构造Merkle数。

[0029] (4)填充其他字段，获得完整区块头。

[0030] (5)CPOW运算，在动态非线性工作量证明机制中，根据当时的时间点往回推算N-1个区块，每一个参与的矿工依照此N-1个区块中获选位验证者的次数，对区块头进行CPOW运算。动态调整其在当时挖矿的困难度，也就是调整工作量证明的期望值大小。

[0031] (6)验证结果，如果符合难度，则广播到全网，挖下一个块；不符合难度则根据一定策略改变以上某个字段后再进行CPOW运算并验证。

[0032] 由于所有的交易数据都会在区块链中显示，于是矿工皆可以轻易计算出其他矿工在某个时间点的困难度为多少，因此动态的调整是可实现的。透过马科夫链的模拟。考虑所有获胜可能性的分布及转换关系，并且比较各种非线性模型后，该发明才用指数模型公开集体验证算法。若两个矿工验证次数差了k次，则验证次数较多的矿工其工作量证明困难将

会是另一个矿工的d的2次方倍。

[0033] 通过改进当前的主流的POW共识机制，加入算力认证部分，可以极大地保护某些具有特定需求的区块链网络。

[0034] 综上所述，基于区块链CPOW共识算法的智能合约网关不仅解决了比特币生态和以太坊生态的兼容性问题，而且解决了区块链的51%攻击问题。

[0035] 基于区块链CPOW共识算法的智能合约网关解决现在比特币生态和以太坊生态系统有的问题和打通两条区块链，将真实商业社会与区块链世界连接。

[0036] 基于区块链CPOW共识算法的智能合约网关可以对接各种应用，比如：互联网金融、网络安全、版权保护等等。

[0037] 互联网金融：基于区块链CPOW共识算法的智能合约网关，能够从根本上修复和重建互联网，其所依托的区块链是一种新型去中心化协议系统，它能安全地储存交易或其他数据，并且无需任何中心化机构审核，因为这些是由整个网络来检验的，那些交易不一定是金融交易，数据也不一定是货币，基于区块链CPOW共识算法的智能合约网关能够被应用在许许多多应用中去。在固有区块链安全的基础上，提升了运行速度，使底层和应用层对接更加方便快捷，有利于维护互联网金融安全。区块链技术是一种以大数据共享理论为基础的现代互联网金融技术，依靠其去中心化、去信任化、集体维护、可靠数据库四大优势，建立金融黑白名单，进而从根本上改变现代金融的征信体系，降低金融风险与金融诈骗风险。区块链技术能够避开繁杂的系统，在付款人和收款人之间创造更直接的付款流程，不管是境内转账还是跨境转账，这种方式都有着低价、迅速的特点，而且无需中间手续费。

[0038] 网络安全：虽然区块链的系统是公开的，但其核验、发送等数据交流过程却采用了先进的加密技术。这种技术不仅确保了数据的正确来源，也确保了数据在中间过程不被人拦截。如果区块链技术的应用更为广泛，那么其遭受黑客袭击的概率也可能会下降，因此人们认为区块链系统要比传统系统更为稳妥。区块链系统之所以能降低传统网络安全风险，一大原因就是它解除了对中间人的需求。

[0039] 版权保护：基于区块链CPOW共识算法的智能合约网关，对版权保护提供了强有力的安全支持。区块链版权之所以能保护原创，是因为它能解决目前原创环境下最迫切的痛点，它在现下的所有版权维权场景中都能适用，因而具有一定的法律效力。区块链版权登记相当于利用区块链去中心化的技术特征，为原创作品嵌入16进制的密码，这个密码会同时储存在区块链的所有电脑上，即相当于为原创作品登记了一张“电子身份证”，且永久有效，无法篡改。

[0040] 本发明基于区块链CPOW共识算法的智能合约网关，不仅有利于不仅节约了研发区块链底层的成本，提供了安全支持，而且每秒数据运行速度也大幅度提升。

[0041] 本发明从协议层出发将开发目标指向应用层提出了基于区块链CPOW共识算法的智能合约网关。以解决比特币生态和以太坊生态的兼容性问题，解决现在区块链两大系统有的问题和打通两条链，设计出更好连接真实商业社会和区块链世界的基础链。

[0042] 本发明提出了CPOW共识算法，通过调整每个矿工获选为验证者的困难度，以解决区块链的51%攻击问题。在比特币POW的基础上采用动态非线性工作量证明机制，在动态非线性工作量证明机制中，根据当时的时间点往回推算N-1个区块，每一个参与的矿工依照此N-1个区块中获选位验证者的次数，动态调整其在当时挖矿的困难度，也就是调整工作量证

明的期望值大小。调整每个矿工获选为验证者的困难度，避免趋向独占验证的可能性，解决了51%攻击的问题。而且缩短了平均区块的确认时间，目标区块创建时间为15s，而比特币的平均区块创建时间是10分钟，大幅度提升了每秒交易的性能，相当于原本比特币每秒交易的40倍。

[0043] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步的详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

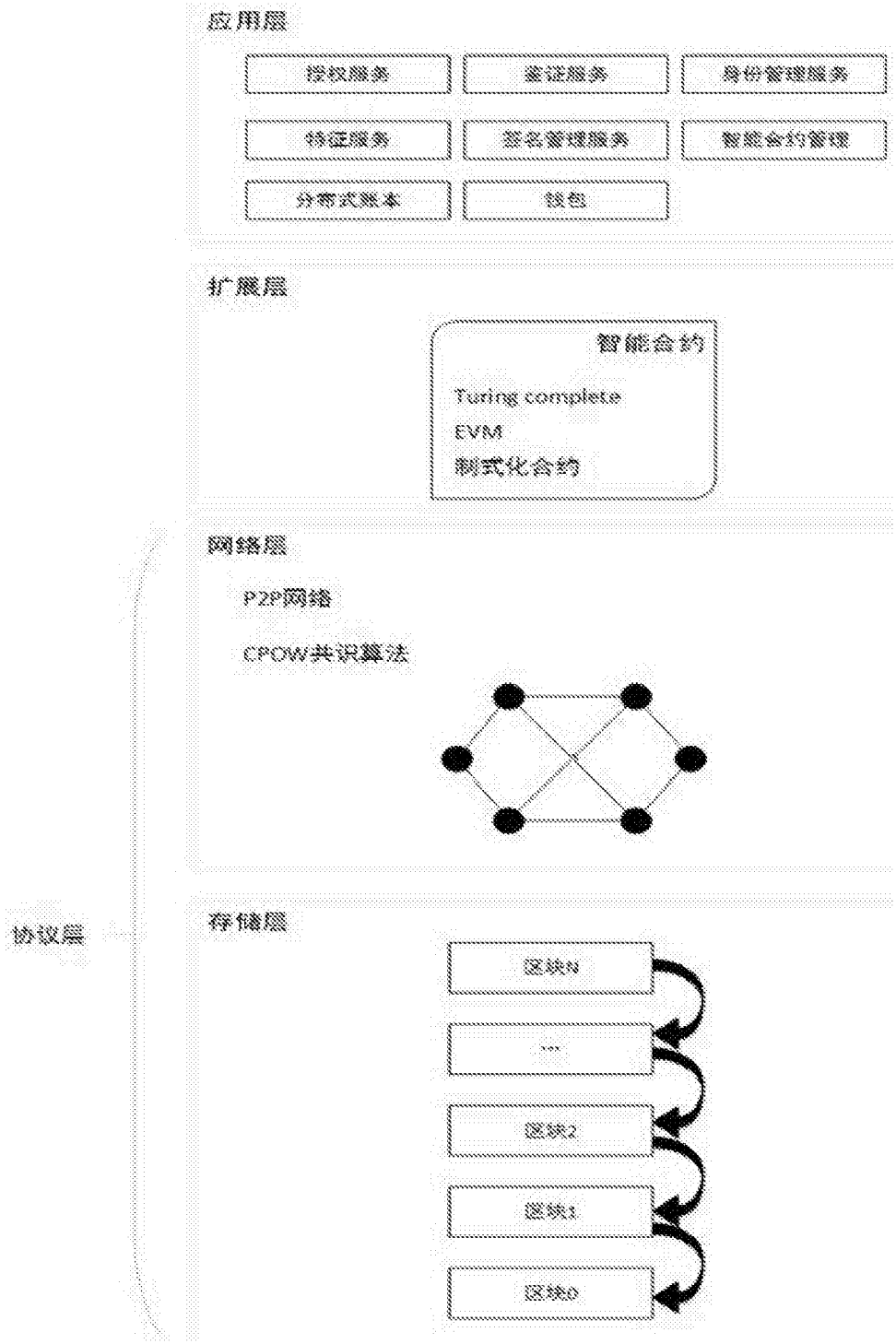

应用层
授权服务
鉴证服务
身份管理服务
存证服务
签名管理服务
智能合约管理
分布式账本
钱包
扩展层
智能合约
Turing complete
EVM
脚式化合约
网络层
P2P网络
CPOW共识算法
协议层
存储层
区块N
...
区块2
区块1
区块0

图1

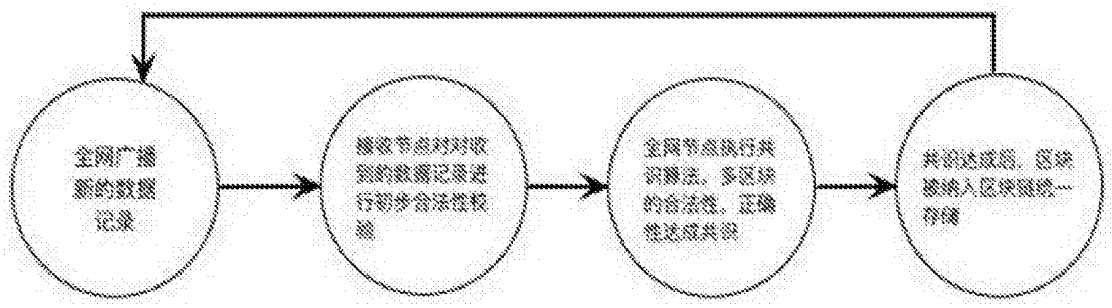

全网广播新的数据记录
接收节点对对收到的数据记录进行初步合法性校验
全网节点执行共识算法，多区块的合法性、正确性达成共识
共识达成后，区块被纳入区块链统一存储

图2