基于附链的容迟网络区块链贸易机制

訾玲玲，丛鑫
（辽宁工程技术大学电子与信息工程学院，辽宁 葫芦岛 125105）

摘 要：为了在非持续连通的容迟网络部署区块链，设计了可运行于该网络的区块链贸易机制。首先，将标志位引入现有的区块数据结构上，提出了可用于追加网络非联通状态生成区块的附链存储结构；其次，提出了附链区块贸易打包方法、挖掘方法和共识方法；最后，提出了避免附链追加过程中区块欺诈的确认共识方法。通过理论证明和实验分析可知，提出的机制可实现在容迟网络中支持区块链贸易。

关键词：区块链；容迟网络；确认共识；贸易机制
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020234

Blockchain trading mechanism based on attached chain for the delay tolerant network

ZI Lingling, CONG Xin
School of Electronic and Information Engineering, Liaoning Technical University, Huludao 125105, China

Abstract: In order to deploy a blockchain on the non-continuous connectivity delay tolerant network, a blockchain trading mechanism was designed, which could run on this type of network. First, the identifier was introduced into the existing block structure and a block structure on the attached chain was presented, which could append the blocks generated during network disconnection. Then, the approaches including the block package, block mining and block consensus on the attached chain were proposed. Finally, a confirming consensus approach was presented to avoid block fraud in the process of appending the attached chain. Through theoretical proof and experimental analysis, the proposed mechanism can support blockchain trading in the delay tolerant network.

Key words: blockchain, delay tolerant network, confirming consensus, trading mechanism

1 引言

区块链技术能使相互之间不信任的用户在不依赖可信第三方的情况下进行安全贸易[1]，其核心优势在于非中心化，通过使用数据加密、分布式共识机制、激励机制，改变了中心化贸易方法，有效地避免了当前贸易过程中的高成本、低效率和不安全数据存储等缺陷。近年来，以太坊的快速发展促进了学术界和工业界对区块链技术开展了新一轮的研究和部署[2-6]，但已有的研究均建立在区块链能运行在持续联通网络的条件下，未涉及网络在非持续联通（如容迟网络）状态下如何利用区块链技术进行贸易。

已有的调查发现，2019 年 53.6%的全球用户都已接入互联网中[7]，通过固定宽带和移动网络接入互联网的分别占 14.5%和 83%，然而，尚有近 67.1 亿人没有接入或者非实时接入互联网。已有的临时网络和容迟网络利用偶发连接可以为非实时情况提供一定质量保证的接入服务，但不能满足区块链运行的需求。如果使远离城市的山区、乡村或者海

收稿日期：2020–07–14；**修回日期**：2020–10–26
通信作者：丛鑫，chongzi610@163.com
基金项目：国家自然科学基金资助项目（No.61702241, No.61602227）
Foundation Item: The National Natural Science Foundation of China (No.61702241, No.61602227)

岛上的居民加入区块链网络开展贸易和挖矿活动，网络接入服务和区块链技术的支持是 2 个必不可少的前提。

对于网络接入服务，可以采用一些服务提供商提供的社区基站方案来解决，对内可为本地的用户搭建社区局域网络，对外通过卫星接入互联网，可提供有时延的网络接入服务。Blattman 等[8]建立容迟网络为偏远山区、海岛等提供远程互联网接入服务。以容迟网络为基础，Hu 等[9]提出了基于以太坊的时延支付方案，重点关注了网络中断情况下生成的数据总量与节点带宽对区块上传的影响。Alaslani 等[10]研究了物联网中影响区块链贸易时间的因素，计算了物联网节点之间采用区块链进行贸易的时延。但上述 2 个文献均未对区块链在该网络下的适应性做表述。对于区块链技术，加密货币的应用使其具有非中心化贸易的特征[11]，但需要持续的网络连接，保证贸易主体和协同者之间进行大量的数据交互。在不能保证实时联通的容迟网络，区块链扩展技术[12]可为区块链部署提供一定的支持，以网络中断为分界，将容迟网络分割为网络联通和非联通 2 个阶段，利用扩展技术将网络非联通时生成的区块在联通时附加到主链上。Worley 等[13]介绍了已有的侧链技术，指出侧链可以有不同于主链的共识协议，但如何有效地将侧链整合到主链上依然是待研究的问题。

综上，如何在容迟网络支持节点之间的区块链贸易是本文解决的问题。本文的贡献如下。

1) 构建了容迟网络区块链贸易模型，以节点能力属性为基准，设计了节点可参与区块链活动的类型，提出了容迟网络区块链贸易的 2 种不同类型及其识别依据。

2) 设计了新的区块数据结构，以此为基础，提出了从属于主链的附链定义、附链区块打包方法、附链区块挖掘方法、附链区块共识方法及网络重联通时附链追加到主链的确认共识方法。

3) 从理论上证明了提出的容迟网络区块链贸易机制具有持续性、安全性和容错性的特征，从实验模拟上分析了所提机制的有效性。

2 容迟网络区块链模型

诺基亚使用 Kuha 基站[14]的方式为难以建立基础通信设施的区域提供周期性网络互联服务。该区域内节点通过基站设备（由 Kuha 提供）实现相互通信，称之为社区，一个社区就是一个局域网络。基站设备与卫星进行连接和通信，为社区内节点提供带有时延的互联网连接服务。与 Kuha 类似，构建带有卫星通信的容迟网络，如图 1 所示。依据节点（用户）所在地理位置将容迟网络分成 2 个表示性的区域：网络实时联通区域（以城市为代表）和网络非实时联通区域（以非城市为代表）。处于实时联通区域的节点很少发生网络中断的情形。位于非实时联通区域基于运营商收益考虑，仅建有少量的基础设施，通过卫星中继接入互联网，其网络连接状态周期性处于非联通状态，该区域内部的节点通过无线或有线方式互通。定义“全网”是指由实时联通区域和处于网络联通周期的非实时联通区域内的节点组成的网络。定义“局域网”是指处于非实时联通区域的连接到同一基站设备的节点组成的网络。假设局域网络为 V，$V=\bigcup_{i\in N} v_i$，N 表示自然数，v_i 表示第 i 个非城市区域。在每个非城市区域内，包含节点和运营商服务器（基站）。

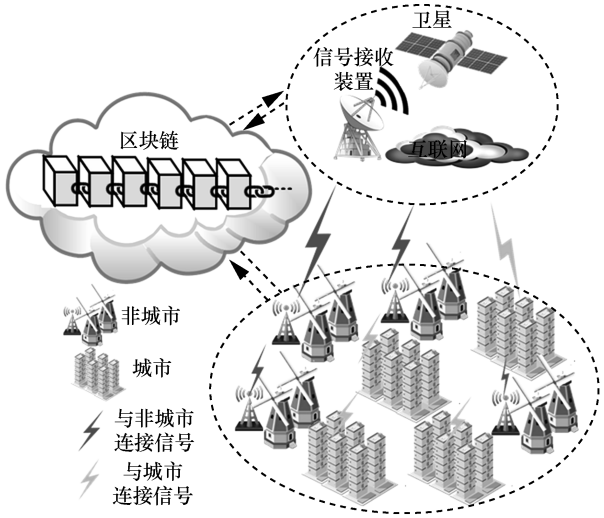

图 1 容迟网络区块链模型

区块链网络建立完成后，可以容纳节点之间的贸易，该网络下的区块链节点活动详细描述如图 2 所示。区块链网络中存在 2 类节点：轻量级节点和完全节点。轻量级节点以手机设备为代表，安装轻量级的区块链软件，具有低计算、存储和带宽能力，在区块链中只能和其他节点发起贸易。完全节点以计算机设备为代表，安装完全的区块链软件，具有一定的计算、存储和带宽能力，在区块链中能进行贸易，参与消息转发、挖矿、共识等活动。考虑非

城市网络会发生连接断开的情况，将贸易类型分为 2 种：贸易发起者在非实时联通区域内，贸易发起者在非实时联通区域外。当网络正常时，区域 v_i 内的节点与其他区域节点一样参与区块链活动，当网络中断时，v_i 内节点在本地设备上记录中断的时间 t_{inter}。设网络重联通时刻为 t_{conn}、t_{inter} 和 t_{conn} 之间的时间段，节点在运营商服务器的支持下会维持封闭的局域 P2P 网络，此时，在该网络中运行区块链应用是可行的。具体来说，位于同一局域网的节点相互之间是可以通过运营商服务器进行相互通信，以此为基础部署区块链，完成对网络非联通状态局域网节点生成贸易记录的打包、挖矿和共识过程。

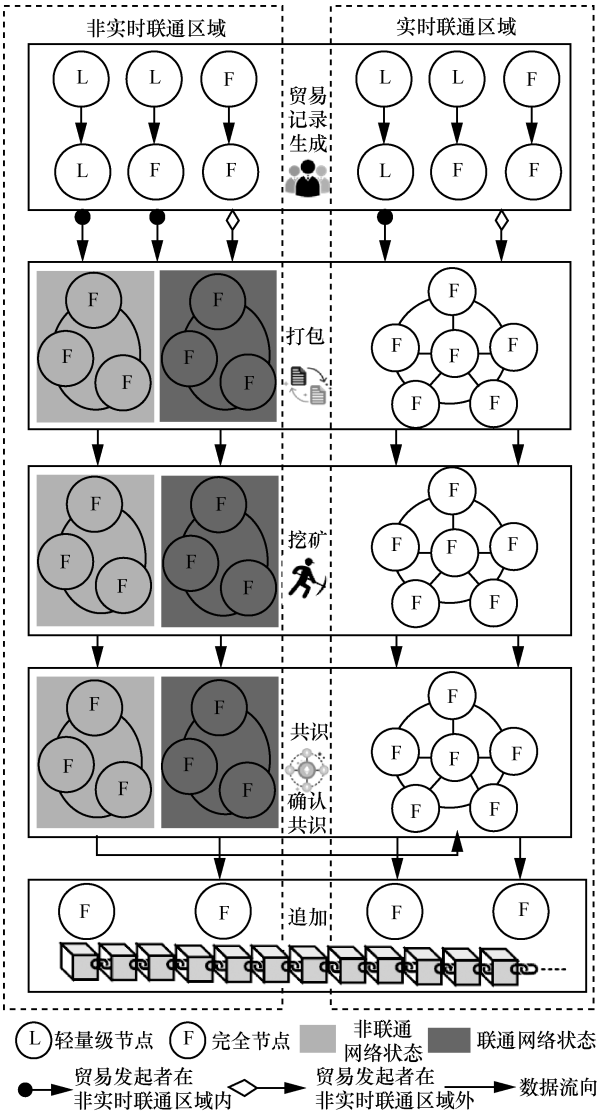

图 2　容迟网络区块链节点活动

如图 2 所示，当前时刻 t（$t_{\text{inter}} \leqslant t \leqslant t_{\text{conn}}$）节点可进行的活动有：1) 继续进行 t_{inter} 之前已经开始的挖矿活动，风险是当网络恢复时，由于时延，该数据块已经被其他节点挖掘出而造成算力浪费；2) 放弃 t_{inter} 之前已经开始的挖矿活动，在本地局域网络内寻找时间戳在 t_{inter} 之后的贸易记录并打包成块，开展挖矿活动；3) 中断当前的验证活动，停止更新本地的区块链账簿，记录中断时区块链最后一块的哈希值。网络连接中断时，在本地局域网络内产生的新贸易记录会被本局域网节点进行打包、挖矿和共识，追加在本地的区块链中。当前时刻 t（$t_{\text{conn}} \leqslant t$）时，网络已经恢复连接，节点可进行的活动有：1) 下载最新的区块链以同步本地账簿；2) 网络连接恢复时将[t_{inter},t_{conn}]周期内追加的区块在整个区块链网络进行确认共识，确认后更新入本地账簿中；3) 未被挖掘的断网时产生的贸易记录全部由本地节点挖掘，网络联通时产生的贸易记录由全网节点挖掘。

3　容迟网络区块链贸易机制

容迟网络在网络中断时形成局域网，网内节点生成的贸易记录只能在局域网内部被接收，节点当前正在进行的挖矿活动会因网络较大的时延而有很大的概率不能追加到区块链上，节点账户信息不能及时更新，从而可能造成虚假贸易，因此局域网生成的区块在网络重联通时需要追加到区块链中且不能对局域网外正在挖矿的节点造成不利影响。针对上述网络非联通情况下的特性和需求，本文修改了附链区块数据结构，将区块链结构更改成可容纳分支的链式结构，设计了附链区块打包方法、挖掘方法、共识方法及网络重联通时的确认共识方法。

3.1　区块数据结构

在企业级网络中，已有的区块链数据结构保证了区块能以链式结构进行分布式存储，但严重限制了区块的可扩展性。为了满足在容迟网络中能利用区块链进行贸易，在主链上容纳网络中断时局域网生成的区块且不对当前正在挖矿的节点产生影响，本文修改了附链区块数据结构，如图 3 所示。

区域 v_i 的网络处于非联通状态时，节点以 t_{inter} 为分界点，通过查询贸易记录时间戳或接收到该贸易记录的时刻将贸易记录分成 2 类：t_{inter} 之前的贸易记录和[t_{inter}, t_{conn}]范围的贸易记录。以此为基础，可采用 3 种方案对贸易记录进行打包成区块：全部打包 t_{inter} 之前的贸易记录；全部打包在[t_{inter}, t_{conn}]范围的贸易记录；混合打包以上 2 种贸易记录。第

一种和第三种方案在网络重联通时，由于较长的时延，有极大的可能性导致该块不能被追加到区块链主链上，虽然浪费算力，但能获取到挖矿的奖励。第二种方案在网络重联通时以附链的方式追加到主链，由于该挖矿属于区域内的活动，没有挖矿奖励，但收取贸易记录内声明的贸易手续费。

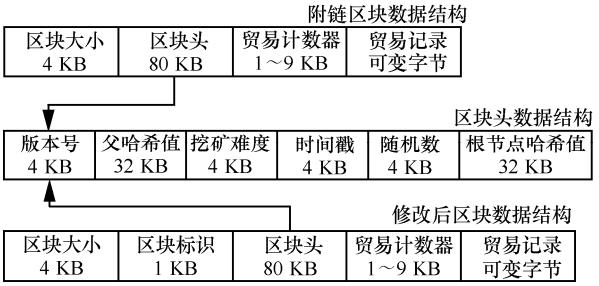

图 3 附链及修改后的区块数据结构

区域 v_i 内节点将贸易记录按图 3 修改后的区块数据结构进行打包成区块，将区块标识位置 1，说明该块是网络处于非联通状态时挖掘出来的，且附加到主链上。将区块标识位置 0，说明该块是网络联通状态下挖掘出来的，参与全网区块共识，确定是否追加到主链上，如果在网络非联通情况下将区块标识位置 0，则由于网络中断时延，有很大的可能性导致该块不能被追加到主链上。网络非联通情况下，父哈希值数据来源于网络中断时本地区块链最后一个区块的哈希值。挖矿难度可以依据区块链更新难度的方式，从网络中获取。

3.2 附链区块挖掘

附链区块挖掘是在容迟网络非联通阶段内由局域网内部节点进行的区块生成的活动，与比特币网络挖矿方法相同。在图 3 所示的区块数据结构下，在一次非联通阶段只能生成一个区块，因此需要依据上一次挖矿时间对挖矿难度进行动态调整。挖矿难度计算方法为

$$\mathrm{BDIFF}=\frac{\mathrm{BMAX}}{\mathrm{BT}}\frac{\mathrm{TA}}{\mathrm{TI}}\frac{\mathrm{CA}}{\mathrm{CI}} \tag{1}$$

其中，BDIFF 是当前的挖矿难度；BMAX 是初始数值；BT 是当前挖矿的目标值；TA 是全网平均挖矿时间，即块生成时间（当前比特币网络块生成时间约为 10 min）；TI 是网络非联通时间；CA 是区块链网络平均算力；CI 是非联通网络节点的平均算力。运营商服务器负责管理 v_i 内节点网络接入功能，可按照全网算力的测算方法统计出网内节点的平均算力 CI，预估网络非联通时间 TI，运营商服务器检测本次网络非联通时间内局域网节点挖矿的区块数（可通过需要共识的区块数确定），初始设置 CI=CA、TI=TA，此时，局域网挖矿难度和全网一致，记录局域网节点挖出的第一个区块的时间，该时间为 TI，统计出全网挖矿的平均时间 TA 和平均算力 CA，即可计算出 CI 值。然后依据每次网络非联通时节点挖掘出的第一个区块的时间动态调整 BDIFF 数值，运营商服务器在网络非联通时将该值广播到所在区域节点，区域内节点就按照此难度值进行挖矿。

3.3 附链区块共识

网络非联通情况下的局域网共识机制与工作量证明类似，需要检查区块标识位是否置 1，若非 1 则放弃该块共识（即使是网络联通正常时挖掘出的区块，即区块标识位为 0，也会因为共识节点比例不够而被放弃，从而浪费算力）；检查难度设置是否与本地难度一致；按照工作量证明进行验证，需要注意的是，节点没有挖矿奖励，仅收取贸易处理手续费。网络非联通状态下附链区块共识算法可简述为：步骤①，验证区块标识，是否为网络非联通时生成的区块；步骤②，验证挖矿难度；步骤③，统计该区块被验证通过的次数（达到区块被全网节点验证通过的比例），具体如算法 1 所示。

算法 1 网络非联通条件下附链区块共识算法

输入 挖掘出的区块

1) 接收其他节点挖掘出来的区块
2) if(区块标识=1) then//步骤①验证通过
3) if(区块挖掘难度=本地接收的难度) then //步骤②验证通过
4) 对比本地接收到的区块，找到时间戳最小的区块
5) 以 PoW 方式对该区块进行验证
6) if(验证通过) then
7) 区块合法
8) 将该区块验证结果广播到网络
9) else
10) 区块非法
11) 放弃该区块
12) end if
13) else //步骤②验证未通过
14) 区块非法
15) 放弃该区块
16) end if

17) else//步骤①验证未通过
18) 区块非法
19) 放弃该区块
20) end if
21) 接收其他节点对该区块的验证消息
22) if(消息数达到设定的阈值) then//步骤③
23) 将该区块以附链的形式追加到本地区块链中
24) else//步骤③小于验证通过的比例
25) 区块非法
26) 放弃该区块
27) end if
28) 网络联通时将该区块广播到全网

网络非联通状态下挖掘的区块可能存在 2 个问题：1)区块造假，节点由于网络非联通状态下挖矿的难度较低，且参与共识的节点相对较少的特征，在网络联通时，私自传播区块，占用网络带宽且浪费算力；2)虚假贸易，用户利用贸易时延，超出账户余额进行贸易，例如用户 John 账户余额为 4 虚拟币，在网络联通时，John 将 3 虚拟币给用户 Bob，该贸易未追加到区块链主链中，在网络非联通时，John 将 2 虚拟币贸易给用户 Alice，这 2 条贸易均可能成功被记录到区块链。为了解决上述问题，在附链区块追加到主链时，需要进行确认共识。

3.4 附链区块追加

网络非联通状态下经共识后的区块，暂时存储在局域网节点处，在网络联通时，每个节点将该区块广播到全网中。接收到该区块的节点，利用哈希函数计算该区块的哈希值，并临时存储在本地，按照预定的阈值，当接收相同哈希值的区块次数超过阈值时，认为该区块为非虚假区块，解决第一个问题。网络中的节点在检查区块真实性后，将该区块每条贸易发起人的账户余额与区块链账簿中该用户的账户余额进行对比，以确定该区块是否有虚假贸易，解决第二个问题。附链区块追加算法（即确认共识算法）可简述为：步骤①，验证区块标识；步骤②，验证同一区块验证次数；步骤③，验证区块内贸易记录，具体如算法 2 所示。

算法 2 确认共识算法

1) 输入其他节点发送的标识位为 1 的区块
2) 接收其他节点发送的待验证的区块
3) if(区块标识=1) then//步骤①网络非联通时生成的区块
4) 计算该区块的哈希值
5) if(该区块哈希值已经存在本地)
6) 该区块接收次数加 1
7) else
8) 计算并验证区块头各项数据是否正确,正确则转发该区块}
9) end if
10) if(一段时间内发送同一区块的不同节点个数达到阈值) then//步骤②
11) 检查该区块内贸易记录，确认贸易人及贸易金额
12) 以本地账簿为准，查询该贸易人余额
13) for(所有贸易记录的贸易人)do//步骤③{
14) if(余额大于贸易金额) then
15) 接收其他节点对该区块的验证消息
16) if(消息数达到设定的阈值) then
17) 区块合法
18) 将该区块作为附链追加到本地区块链中
19) else //消息数小于阈值
20) 区块非法
21) 放弃该区块
22) end if
23) else//余额小于贸易金额
24) 区块非法
25) 放弃该区块
26) end if
27) end for
28) else//步骤②节点接收同一区块次数小于阈值
29) 区块非法
30) 放弃该区块
31) end if
32) else//步骤①网络联通时生成的区块
33) 按 PoW 方式进行共识
34) end if

4 理论分析和性能评估

评定区块链性能的基本属性包括持续性和安全性[15-16]。持续性保证了区块链服务的可用性，安全性保证了在同一时刻有且仅有一个区块能被节点接收。评定区块链性能的扩展属性为容错性，保证区块链服务可正常工作条件下，网络中容许恶意

节点的比例。

依据文献[15,17]，区块预期生成时间 B_{time} 符合指数分布，其密度函数为 $\kappa \mathrm{e}^{-\kappa B_{\text{time}}}$，$\kappa$ 为常数，区块链网络 $\kappa=0.079$，以太坊网络 $\kappa=0.083$。在区块链中，将时间分割成时间段，以节点接收到新的区块的时间为界，界前时间为前一区块计时的终止，界后时间为当前区块计时的开始。按照区块链运行协议，在当前时间段内，节点接收到时间戳为 TS 的新区块，该节点应该依据算法 1 验证该区块的有效性，验证成功后，停止当前的挖矿活动，在 $\mathrm{TS}+\tau$ 时间内持续监听和接收更多的新区块。τ 是接收新生成块的等待时间。依据上述描述，本文分析设计的区块链的性能。

4.1 理论分析

定义 1 持续性。在每个时间段内，生成至少一个新的区块。

定义 1 处于非联通状态下的容迟网络，在不超过 $\dfrac{\tau}{\mathrm{TR}_{\text{total}}}$ 时间内至少生成一个新区块。
$\sum_{i=1}\mathrm{TR}_i$

证明 在区块链中，矿工将多条贸易记录打包成区块，以达到预期的收益。依据 B_{time}，在一个时间单位内，会有多个贸易记录到达矿工节点。在 τ 内，贸易手续费满足 $\sum_{i=1}^{\mathrm{TR}_{\text{total}}}\mathrm{TR}_i$ 的贸易被矿工打包，则生成下一个区块的时间为 $\dfrac{\tau}{\sum_{i=1}\mathrm{TR}_i}$。因此，矿工通常在 $\dfrac{\tau}{\mathrm{TR}_{\text{total}}}$ 时间内生成一个新的区块。
$\sum_{i=1}\mathrm{TR}_i$

证毕。

定义 2 安全性。在每个时间段内，即使由不同的矿工生成多个区块，也不会产生分支。

定义 2 处于非联通状态下的容迟网络，假设标号为 0~N 的区块已经追加到区块链中，在下一个时间段内，遵守区块链协议的矿工会共识同一标号为 N+1 的区块。

证明 依据定义 1，在标号为 0~N 的区块被追加至区块链后，在一个时间段内，有至少一个标号为 N+1 的区块由矿工生成。在新区块生成的同时，矿工会将该区块立刻广播到网络中，而在有限时间内，该区块就会被网络中其他节点接收到。假设节点 i 在 t_0 时刻接收到该时间段内的第一个区块 B_{N+1}，则 i 在 $t_0+\tau$ 时间内持续监听和接收其他区块。$t_0+\tau$ 时刻之后，依据算法 1，i 选择时间戳最小的区块作为标号为 N+1 的区块加入到区块链中。

依据以上过程，网络中的节点都依据自己接收的新区块，确定标号为 N+1 的区块，该区块的时间戳为 TS_{N+1}，且 $t-\mathrm{TS}_{N+1}>0$，有式(2)所示密度计算式成立。

$$f\left(t_0=t\right)=\kappa \mathrm{e}^{-\kappa\left(t-\mathrm{TS}_{N+1}\right)} \tag{2}$$

则有

$$P\left(t_0<t\right)=1-\mathrm{e}^{-\kappa\left(t-\mathrm{TS}_{N+1}\right)} \tag{3}$$

在一段时间结束时，即 $t=\mathrm{TS}_{N+1}+\tau$ 时刻，标号为 N+1 的区块被节点接收的概率为

$$P\left(t_0<t\right)=1-\mathrm{e}^{-\kappa\tau} \tag{4}$$

由式(4)可以得到，当时间戳大于 TS_{N+1} 的区块到来时，其监听持续时间 t'要小于 $\mathrm{TS}_{N+1}+\tau$，依据概率论的置信区间原则，该区块被接收的概率降低，即

$$P\left(t_0<t'\right)<P\left(t_0<t\right)=1-\mathrm{e}^{-\kappa\tau} \tag{5}$$

接收新区块的等待时间 τ 是影响区块被接收概率的关键参数，该参数可依据网络状态和实际需求进行动态调整，可取值为 $\tau=12\omega$（以太坊区块链）或 $\tau=12.6\omega$（比特币区块链），$\omega\in[1,10]$。当 $\omega=2$ 时，时间戳为 TS_{N+1} 的新块被接收的概率为 0.865；当 $\omega=6$ 时，时间戳为 TS_{N+1} 的新区块被接收的概率为 0.99。

证毕。

定义 3 容错性。在区块链网络中存在恶意节点的情况下，遵守区块链协议的节点也能将同一区块追加到区块链中。

定义 3 处于非联通状态下的容迟网络，一定比例的恶意节点不会对新区块的追加造成影响。

证明 基于区块链中节点不可信及以利益为驱动的事实，理性的恶意节点也是以获取更多收益为目标。根据定义 2，一旦恶意节点较之其他节点先挖掘出区块，该节点会在第一时间将该区块广播到全网，以取得较大的接收概率，此时恶意节点不会有恶意行为，也不会对区块追加造成影响。反之，该节点会与其他恶意节点联合，以使挖掘的区块被接收。然而，遵守区块链协议的节点由于该区块时间戳较大而拒绝接收该区块。

当节点不确定接收到的区块来源是否是恶意节点时，节点可以向其他节点发送请求，以更新本地接收到的区块。如果被请求的节点中有遵守区块链协议的节点，则该节点能得到本时间段有最小时间戳的区块，从而保证恶意节点不会对该节点追加的新区块造成影响。

但存在一种极端情况，即节点发送更新区块请求时，其邻居节点均是恶意节点，此时，更新的区块是错误的，会影响新区块追加。假设区块链网络中的节点数量为 O，恶意节点数量为 Ω，则恶意节点的比例 $\psi=\dfrac{\Omega}{O}$。设节点的邻居数量为 H，则邻居节点均为恶意节点的概率 Π 的计算方法可简述为第一个邻居节点为恶意节点的概率为 $\dfrac{\Omega}{O}$，第二个邻居节点为恶意节点的概率为 $\dfrac{\Omega-1}{O}$，依次类推，第 H 个邻居节点为恶意节点的概率为 $\dfrac{\Omega-H+1}{O}$，则有

$$\Pi=\frac{\Omega}{O}\frac{\Omega-1}{O}\frac{\Omega-2}{O}\cdots\frac{\Omega-H+1}{O} \tag{6}$$

依据网络实际需求，设最大可容纳恶意节点的比例为阈值 σ，Π 要满足不大于 σ，即

$$\psi\left(\psi-\frac{1}{O}\right)\left(\psi-\frac{2}{O}\right)\cdots\left(\psi-\frac{\Omega-1}{O}\right)\leqslant\sigma \tag{7}$$

在网络中，节点的邻居节点数量和网络中全部的节点数量的比值趋近于 0，式(7)可以近似转换为

$$\psi^{H}<\sigma \tag{8}$$

从式(8)可知，H 越大时，Π 越小，但 H 值影响设备的性能，即设备同时连接节点数是有限制的。当 $\sigma=1\times10^{-6}$、平均邻居节点数为[10, 20]，网络中可以容纳的恶意节点比例为 25%~50%。

证毕。

定义 4　能耗。能耗是指区块生成过程中的电力消耗。相比于 PoW 方式，在全网范围内生成主链区块的能源消耗变化不大。在局域网范围内由于算力相对于全网来说是有限的，依据设计的挖矿难度动态调整算法，生成附链区块所消耗的电力较低。

定义 5　区块生成时间和确认时间。区块生成时间是指从贸易记录打包开始，直到区块被挖掘出来为止。确认时间是指从区块生成时刻算起到追加到区块链上为止。相比于 PoW 方式，在全网范围内主链区块生成时间和确认时间变化不大。在局域网范围内依据挖矿难度动态调整算法，附链区块生成时间较短。但附链区块需要在局域网络联通时上传到全网其他节点进行确认共识，确认共识时间与 PoW 一致，上传时间取决于网络带宽，因此，附链区块确认时间较 PoW 长。

4.2　性能评估

为了评估所提机制在网络非联通状态下的性能，利用 PeerSim[18]模拟器建立 P2P 网络环境用以运行区块链系统，并将该网格分割成多个封闭的 P2P 子网络，每个子网络设置主路由节点模拟运营商服务器，主路由节点的工作方式是周期性地连接或断开局域网络，以模拟基站与卫星的工作方式。区块链运行协议为区块链协议，数据传输遵循 TCP/IP（transmission control protocol/Internet protocol）。使用由 10 台刀片式服务器组成的服务器集群作为硬件运行环境，每个刀片服务器的主要配置为 2 颗 Intel Xeon E5-2620 CPU，每颗包含 8 核、16 线程、32 GB 内存。由这些服务器集群利用虚拟化方式生成 1 000 个节点，每个节点的算力相同，初始区块生成时间为 10 min，按照已有的矿机的收益和成本参数，设置区块中的虚拟货币（收益）和实际的美元（成本）的比值 ζ 的数量级为 10^{-4}，网络中断时间和网络联通时间的比值为 0.5。依据文献[17,19]，贸易到达速率符合参数为 0.079（即比特币 $\dfrac{1}{12.6}$）的泊松分布。定义节点的收益率 B_{rate} 为节点的收益和成本的比值，即

$$B_{\text{rate}}=\frac{\text{Income}-\text{Consume}}{\text{Consume}} \tag{9}$$

其中，Income 是挖矿获得贸易的处理费用，是一段时间内挖矿成功时获得的费用之和；Consume 是付出的成本，包括电费、设备费等，是一段时间内无论挖矿是否成功都要付出的成本之和。节点打包贸易记录采用的方法有 2 种：1) 将每条贸易的处理费用按从高到低排序，选择前面的贸易记录打包；2) 在 1)的基础上，随机附加贸易处理费用低的贸易记录打包。

长时间运行的非联通网络区块链节点的收益率变化如图 4 所示。从图 4 中可以看出，节点的收益率在运行过程中是稳定的，这是由于节点能依据上次挖矿时确认共识的结果调整本次打包的记录个数，从而保证确认共识时需要的区块能成功广播

到全网。当区块中的货币实际价格升高时，在保证收益的情况下，节点采取降低打包的贸易记录条数，减少区块的大小，较稳妥地获得该区块的收益。

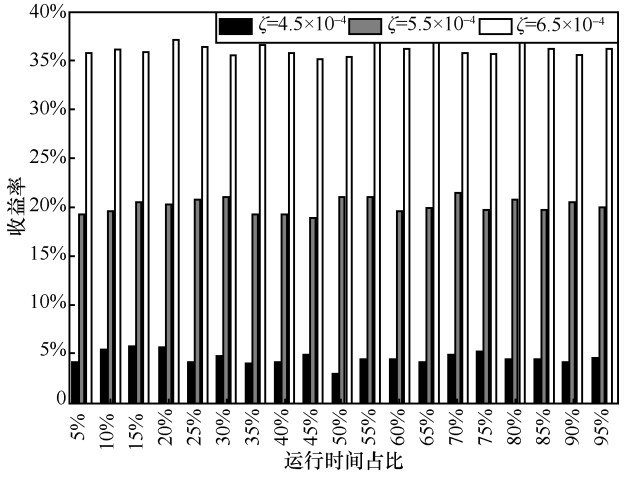

图 4 非联通网络区块链节点的收益率变化情况

图 5 显示的是贸易个数和收益率之间的关系。贸易个数反映的是区块在非联通网络高带宽节点比例固定（25%）的情况下的大小，理论上讲，贸易个数越多，则获得的收益越大。但实际上，当贸易个数过多（区块较大）时，会在网络联通时没有足够的节点成功将该区块广播到全网中，导致算法 2 中节点接收同一区块数达到阈值这一条件不能满足，致使该区块被放弃，不能获得收益。从图 5 中可以看出，收益率随贸易记录数的增加存在最大值，该值之后的区块广播会存在一定的失败概率。当挖掘出来的区块大小和区块大小上限的比例超过 75%时，区块广播成功率会急剧下降，导致负收益的情况发生。

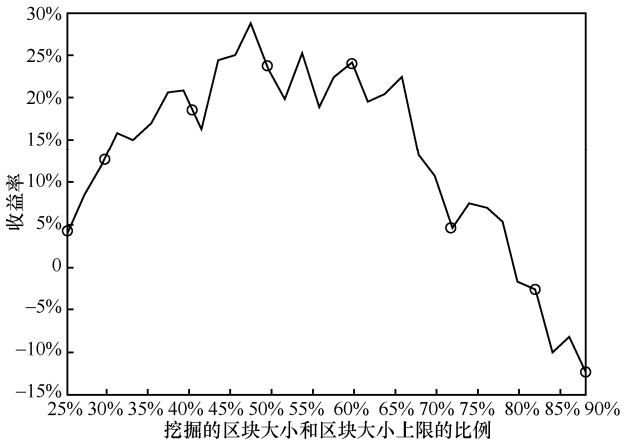

图 5 贸易个数的增加对收益率的影响

网络时延和难度级别的关系如图 6 所示，其中纵坐标是调整后的挖矿难度与当前比特网挖矿难度的比值。网络时延和网络非联通时间相关，非联通时间越长，网络时延越大。依据一条附链只能附加一个区块的原则，当网络时延较大时，适当调整挖矿难度只能在同一网络非联通时段挖掘出一个区块。

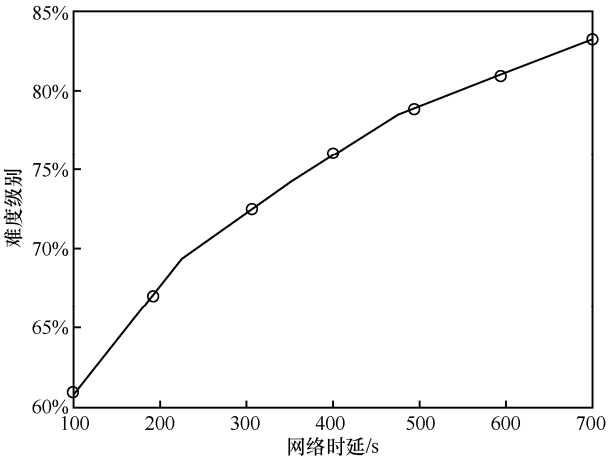

图 6 网络时延和难度级别的关系

在相同网络时延下，网络中恶意节点数量对区块生成时间的影响如图 7 所示。当网络中恶意节点的比例分别为 10%、25%、40%时，区块生成时间变化不大，也就是说，一定比例恶意节点的存在不会对贸易和区块生成造成很大的影响，这与定义 3 的结论相一致。

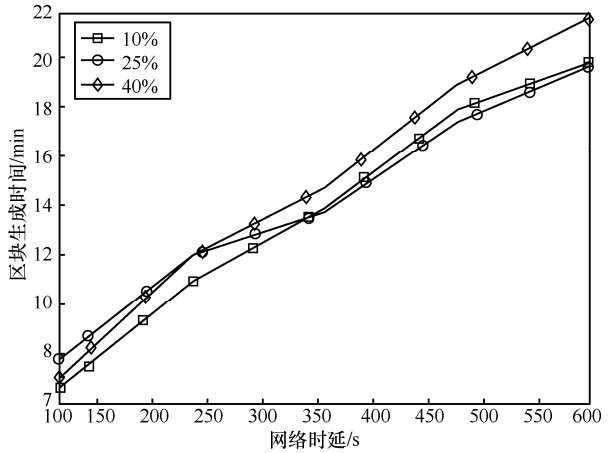

图 7 恶意节点比例对区块生成时间的影响

5 结束语

目前的区块链只能在实时联通的网络环境下部署和进行贸易，但对诸如容迟网络的非实时联通

网络提供支持却无能为力。本文研究了如何在容迟网络进行区块链贸易的问题。将容迟网络分为非联通和联通 2 个状态，在非联通状态，修改了现有的区块数据结构，提出了附链的概念，详细介绍了附链的贸易记录打包成区块的方法，基于难度动态调整的附链区块的挖掘方法和基于标识位的区块共识方法；在网络联通状态，设计了防止区块造假和虚假贸易的确认共识方法。以理论分析和模拟实验为手段，分析了提出的容迟网络区块链贸易机制的有效性，使节点拥有较高的收益率。

鉴于采用 PoW 工作方式的区块链在实际应用中具有明显缺陷，如能耗过高、贸易处理时间过长等，下一步工作从设计公平、安全和高效的矿工选择方法和附链分支处理方法出发，减少区块生成过程中无用的计算及降低区块的生成和确认时间。

参考文献：

[1] MOHANTA B K, JENA D，PANDA S, et al. Blockchain technology: a survey on applications and security privacy challenges[J]. Internet of Things, 2019, 8: 100107.

[2] ZHENG Z, XIE S, DAI H, et al. An overview of blockchain technology: Architecture, consensus, and future trends[C]//2017 IEEE International Congress on Big Data. Piscataway: IEEE Press, 2017, 557-564.

[3] SI H, SUN C, LI Y, et al. IoT information sharing security mechanism based on blockchain technology[J]. Future Generation Computer Systems, 2019, 101: 1028-1040.

[4] LEE H, MA M. Blockchain-based mobility management for 5G[J]. Future Generation Computer Systems, 2020, 110: 638-646.

[5] DI VAIO A, VARRIALE L. Blockchain technology in supply chain management for sustainable performance: evidence from the airport industry[J]. International Journal of Information Management, 2020, 52: 102014.

[6] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理, 进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.

[7] JOSHUA H, KELLY W, MIKE H. Mapping the scope of software interventions for moderate Internet use on mobile devices[C]//Proceedings of the 7th International Conference on ICT for Sustainability. New York: ACM Press, 2020: 204-212.

[8] BLATTMAN C, JENSEN R, ROMAN R. Assessing the need and potential of community networking for development in rural India special issue: ICTs and community networking[J]. The Information Society, 2003, 19(5):349-364.

[9] HU Y, MANZOOR A, EKPARINYA P. A delay-tolerant payment scheme based on the ethereum blockchain[J]. IEEE Access, 2019, 7: 33159-33172.

[10] ALASLANI M, NAWAB F, SHIHADA B. Blockchain in IoT systems: end-to-end delay evaluation[J]. IEEE Internet of Things Journal, 2019, 6(5): 8332-8344.

[11] LEE J Y. A decentralized token economy: how blockchain and cryptocurrency can revolutionize business[J]. Business Horizons, 2019, 62(6): 773-784.

[12] KIM S, KWON Y, CHO S. A survey of scalability solutions on blockchain[C]//2018 International Conference on Information and Communication Technology Convergence. Piscataway: IEEE Press, 2018: 1204-1207.

[13] WORLEY C, SKJELLUM A. Blockchain tradeoffs and challenges for current and emerging applications: generalization, fragmentation, sidechains, and scalability[C]//2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data. Piscataway: IEEE Press, 2018: 1582-1587.

[14] GORARD S, GORARD J. Explaining the number of counterfactual cases needed to disturb a finding: a reply to Kuha and Sturgis[J]. International Journal of Social Research Methodology, 2016, 19(4): 497-499.

[15] MOIN S, KARIM A, SAFDAR Z. Securing IoTs in distributed blockchain: analysis, requirements and open issues[J]. Future Generation Computer Systems, 2019, 100: 325-343.

[16] FENG W, YAN Z. MCS-chain: decentralized and trustworthy mobile crowdsourcing based on blockchain[J]. Future Generation Computer Systems, 2019, 95: 649-666.

[17] DECKER C, WATTENHOFER R. Information propagation in the bitcoin network[C]// IEEE P2P. Piscataway: IEEE Press, 2013: 1-10.

[18] KAZMI I, BUKHARI S. PeerSim: an efficient & scalable testbed for heterogeneous cluster-based P2P network protocols[C]//2011 UkSim 13th International Conference on Computer Modeling and Simulation. Piscataway: IEEE Press, 2011: 420-425.

[19] KASAHARA S, KAWAHARA J. Priority mechanism of bitcoin and its effect on transaction-confirmation process[J]. arXiv Preprint, arXiv:1604.00103, 2016.

[作者简介]

訾玲玲（1981– ），女，辽宁阜新人，博士，辽宁工程技术大学副教授、硕士生导师，主要研究方向为区块链、计算机视觉。

丛鑫（1982– ），男，辽宁阜新人，博士，辽宁工程技术大学高级工程师、硕士生导师，主要研究方向为 P2P、云计算和区块链。