基于命名数据网络的区块链信息传输机制

刘江[1,2]，霍如[2]，李诚成[1,2]，邹贵今[1,2]，黄韬[1,2]，刘韵洁[1,2]
（1.北京邮电大学网络与交换技术国家重点实验室，北京 100876；2.北京工业大学北京未来网络科技高精尖创新中心，北京 100124）

摘 要：近年来关于区块链的研究得到极大关注，然而基于 TCP/IP 的通信对这种大量数据内容广播模式的支撑并不充分。基于命名数据网络，设计全新的支持区块链推送服务的节点模型和特殊的读写表过程，提出完善的信息传输机制，通过请求聚合和数据缓存减少网内冗余流量并加速通信传输。同时给出基于本架构的虚拟货币应用实例，并通过仿真验证本方案性能的优势，进一步展望未来相关的研究方向。

关键词：命名数据网络；区块链；信息推送；内容广播；反向读写表项
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018005

Information transmission mechanism of Blockchain technology based on named-data networking

LIU Jiang[1,2], HUO Ru[2], LI Chengcheng[1,2], ZOU Guijin[1,2], HUANG Tao[1,2], LIU Yunjie[1,2]
1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Beijing Advanced Innovation Center for Future Internet Technology, Beijing University of Technology, Beijing 100124, China

Abstract: Recent researches on blockchain have been greatly concerned by academia and industry, while the communication based on TCP/IP protocol was not enough for broadcasting a large volume of data in blockchain technology. Therefore, a novel node model supporting push service for blockchain technology and a special procedure reading-writing the table of the node model were designed based on the named-data networking, which was a distributed network architecture supporting data transmission naturally. And then the information transmission architecture of blockchain technology via named-data networking was proposed. With the aggregation of the requests and data caching, this architecture could reduce the traffic redundancy and accelerate the communication speed. Meanwhile, a use case of bitcoin based on the proposed architecture was given, in order to better understand the architecture. A numerical simulation was used to verify the performance advantages of the proposed scheme. In addition, some related future research directions were presented.

Key words: named-data networking, blockchain, information pushing, content broadcasting, read and write the table entry reversely

1 引言

2015 年下半年，区块链的概念迅速崛起，全球许多金融机构和相关的 IT 企业掀起了一场在经济和互联网方面区块链技术带来的商机热潮。如果说互联网是实现了信息的传播，那么区块链就是进一

收稿日期：2017-04-20；**修回日期**：2017-12-21
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA016101）；北京市科技新星基金资助项目（No.Z151100000315078）；信息网络领域开源平台及技术发展战略基金资助项目（No.2016-XY-09）；我国未来网络技术、平台、体制创新战略研究基金资助项目（No.2013-ZX-04）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA016101), Beijing New-Star Plan of Science and Technology (No.Z151100000315078), Open Source Platform and Technology Development Strategy of Information and Networks Foundation (No.2016-XY-09), Research on Future Network Technology, Platform and System Innovation Strategy Foundation of China (No.2013-ZX-04)

步实现了价值的转移，可以说区块链技术是互联网后下一代发展的颠覆性技术之一。该技术将某个时间段内的数据存储在一个区块内，不同的区块按照时间顺序就形成了一个链状结构，同时使用非对称密钥和散列算法等密码学方法加密这些信息数据，保证数据的不可篡改和安全性，在没有第三方信任机构的情况下，全网也能达成共识和完全的信任，形成了一个去中心化的分布式数据库。目前，区块链技术不仅在金融行业体现了巨大的应用前景，而且在大数据、物联网、人工智能等信息技术领域也有着互相影响的助力。

区块链技术越火，应用的范围越广，就对这个通信网络的要求越高，从而保证其相关业务的性能。对于这种大量的数据在网络中同步传输的模式，人们希望有更加匹配这种模式的网络架构，来优化区块链技术相关业务的传输。现有的 IP 网络需要 2 个主机端多次握手连接后才能进行后续数据分组的转发，且就广播而言，一个主机如果要将数据广播给网络中的所有 n 个节点，就需要封装 n 个数据分组，分别发送给这 n 个节点，造成统一数据的冗余传输，如果发生分组丢失现象，则更增加网络的负担。在未来网络解决数据传输的网络架构中，命名数据网络（NDN, named-data networking）一直是备受关注的重点研究架构，它作为一个分布式的网络架构，尽管沿用了 IP 网络的沙漏模型，但是却是以内容名字作为“细腰”，实现了基于内容命名的路由和转发，更加符合用户对互联网的直观使用方式。命名数据网络请求聚合和内容缓存的优良特性，能够为区块链技术信息传输提供更好的加速服务并且减轻整个网络的流量负载。

尽管命名数据网络在属性上符合解决区块链技术信息传输问题的思路，但是目前区块链技术是一种基于点对点的主动推送数据的通信模式，而命名数据网络则是一种基于用户主动请求从内容源端拉取内容的网络架构。为了让命名数据网络能够更好地支撑区块链技术的相关业务，本文提出了一种新颖的基于命名数据网络的区块链技术信息传输机制，在原有支持内容分发业务的基础上，引入了推送服务业务，改进了原有的命名数据网络节点模型，当节点收到请求分组后，首先判断请求分组的业务类型，对于推送服务类型的业务，通过设计的推送服务待定兴趣表来进行读写表处理，并且通过反向写表项的过程一次完成由推送方主动发起数据分组推送过程。在这种大量数据传输的区块链技术相关业务中，本文提出的机制可以为这类实时性的推送业务提供加速服务，并减轻整个网络重复的冗余流量传输。

2　区块链技术

2.1　研究背景

区块链由一系列根据时间顺序生成的记录交易数据的区块（block）链接组合形成，构成了系统内所有节点共享的交易数据库。通过区块链技术形成存储的数据具有不可篡改和无法伪造的时间戳，任何交易都有完整的证据链和可信任的追溯环节。区块链技术起源于虚拟货币，2008 年虚拟货币诞生，紧接着，2009 年出现了序号为 0 的虚拟货币创世区块，并与序号为 1 的区块相连形成了链，标志着区块链的诞生[1]。

区块链的宗旨是要去中心化和实现匿名，建立自己系统内公开的信任机制[2]。其信任机制建立在非对称密码学基础上，系统使用者不需要了解对方基本信息即可进行可信任的价值交换，即在没有中心机构的情况下达成共识，提高了传统网络交易的效率。任何人在任何时间都能够通过相同的技术在区块链上录入自己的信息，而区块链在数据透明的基础上对所有交易对象都是匿名存在的，一定程度上保证了私人信息的安全性。它不依赖第三方，而是通过自身分布式节点进行网络数据的存储、验证、传递和交流，解决了传统互联网交易中基于信任而存在的第三方中介运营成本过大、网络信息安全性不高的问题[3]。

区块链技术是具有普适性的底层技术框架，目前，一般认为区块链技术正处于 2.0 模式（可编程金融）的初期，众多如智能合约、电子商务、证券交易、股权众筹、物联网和 P2P 借贷等各类基于区块链技术的互联网金融应用相继涌现，发展前景广阔。未来区块链将更多地应用于如新型宽带网络、保险行业风险评估、艺术交易、法律公证、数字资产等生产、生活中的各个方面。

2.2　区块链技术原理

区块链技术是基于密码学中椭圆曲线数字签名算法（ECDSA）实现去中心化的点对点系统设计，将区块以链的方式组合在一起形成数据结构，以参与者对全网交易记录的事件顺序和当前状态建立共识为基础，存储有先后关系的、能在系统内验证

的数据，并用密码学保证这些数据不可篡改和不可伪造。区块链技术原理如图 1 所示，区块链由一系列按时间顺序排列的区块组成，每个区块由上个区块的散列值与本区块的内容、时间戳、数字签名和共识机制共同组成，对于不同的应用来说，主要体现在存储内容和共识机制不同。

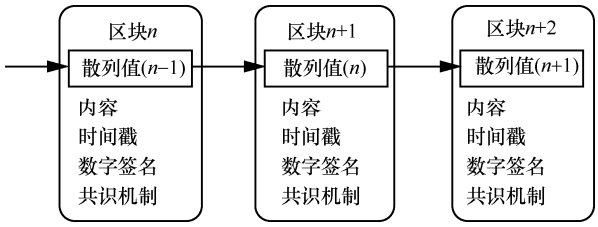


图 1 区块链技术原理

区块链的核心技术主要包括 4 个方面。

1) 区块+链

区块链改进了传统的数据库结构，将数据分成若干区块，每个区块记录着它被创建期间发生的所有交易活动信息，这些区块按照时间的先后顺序链接在一起，形成一个完整且不可篡改的交易数据库，并被系统内的所有节点共享。

2) 非对称加密算法和授权技术

区块链技术的密钥对中的公钥全网公开，所有人都可以用自己的公钥来加密一段内容，验证内容的真实性；私钥只有信息拥有者可知，被加密的内容只有通过相应的私钥才能解密，保证内容的安全性。在区块链应用的交易中，公钥加密交易信息，私钥解密交易信息；同时私钥对信息签名，公钥验证签名，通过公钥签名验证信息可以确认该交易信息是否由私钥持有人发出。整个过程中，交易信息是透明公开的，但账户信息采用纯数学方式高度加密，实现交易匿名，保证隐私安全。

3) 共识机制

由于点对点网络下存在较高的网络时延，各个节点所观察到的事务先后顺序不可能完全一致，因此，区块链技术需要一种机制使所有通信节点对于在差不多时间内发生的事务的先后顺序达成共识。这种对一个时间窗口内事务的先后顺序达成一致的算法被称为共识机制。常用的共识算法类别有工作量证明（POW）、权益证明（POS）、代议制权益证明（DPOS）和过去时间证明（POeT）等。

4) 脚本

一个脚本本质上是众多指令的列表，具有可编程性，这些指令记录着每一次价值交换活动中，交易双方进行交易需要满足的附加条件，而在去中心化的环境下，所有的协议都需要提前取得共识，而脚本的引入就使区块链技术能有机会去处理一些系统中无法预见到的交易模式，增加了该技术的实用性。

2.3 区块链技术优势及需求

区块链技术与金融市场应用有很高的契合度，R3CEV、纳斯达克等各金融机构相继投入区块链技术的研发中。区块链在很大程度上实现了金融脱媒，这对第三方支付、资金托管等存在中介机构的商业模式来说是颠覆性的变革[1]；基于区块链的智能宽带网络也正致力于从集中式转变为分布式，使共享的没有信任关系的网络节点实现安全的信息传输[4]；在医疗方面，区块链的非对称加密技术可以使健康数据被更好地保护起来，防止非正常泄露带来的严重后果，便于建立一个全人类安全的健康数据库；而且在如今发展迅速的物流供应领域，区块链技术能为供应链中的物流信息提供认证服务，通过区块链数据库的源头追踪功能就可以很快地找到问题所在，实时追踪商品流转信息，实现全透明消费[5]。可以预见，未来区块链技术将更多地被应用到人们生活的方方面面。

可以看出，区块链的推广日益增长，随着区块链应用的不断普及，更多的数据会在网络中传输，为了给用户提供更好的体验并且保证应用业务的实时性，如何保证高效良好的区块链信息传输成为未来一个值得研究的问题。在这个问题的研究过程中，要充分考虑到支持分布式网络、支持点对点通信、支持内容推送、很好地支持内容广播、更好地缓解网络信息传输压力等特征。

3 命名数据网络

3.1 研究背景

随着内容的增多和终端设备不断地加入，互联网逐渐由一个传统的端到端通信网络向一个分布式内容分发网络的方向发展。由于在 TCP/IP 网络架构下，IP 地址数量是有限的，这将越来越难以满足日益增多的互联网终端设备，同时基于端到端连接的通信模式将会导致路由条目的急剧增多，增大骨干网的流量压力，原有的“细腰”IP 层将会成为限制网络内容增长、接入设备增多以及网络流量增加的瓶颈。

命名数据网络借鉴并保留了原有 TCP/IP 网络体系架构的沙漏模型，但 NDN 在沙漏模型的“细腰”部位采用了内容块（content chunk），也就是将网络中的内容资源等信息与 IP 地址之间的关系解耦，转而与内容的命名绑定，将网络的关注点从“在哪里”转变成“是什么”，适应了当前互联网对内容需求不断增加的趋势。NDN 属于信息中心网络（ICN, information-centric networking）中分布式架构的代表，即 NDN 中的每一个节点都拥有全网的状态信息，可以独立地实现路由计算、路由选择以及转发。此外，ICN 体系中还有集中式架构，主要有面向数据的网络体系架构[6]、发布/订阅式网络体系架构[7,8]等，这些架构以集中式路由选择策略为核心，由网络控制系统收集全网状态信息并实现路由计算和路由选择。在经历概念提出、协议栈定义、数据结构与关键技术设计以及命名链路状态路由协议[9]的设计之后，目前，NDN 项目组将研究的重点放在 NDN 转发守护进程[10,11]上，并且基于上述的研究完成了一张全球范围的 NDN 试验床的搭建工作，并在不断地更新与维护。

此外，学术界和产业界也在积极地将 NDN 与物联网、车联网等概念进行结合，希望将 NDN 内容分发的优势运用到现有的网络中。

3.2　命名数据网络通信模型

NDN 中交互的分组分为 2 类，分别是 Interest（请求）分组和 Data（数据）分组。NDN 作为请求方驱动的网络，Interest 分组是由内容请求方向内容源发出的、用于请求相应内容的请求分组；Data 分组则是由内容源或内容缓存节点返回的内容。命名数据网络单个节点通信流程如图 2 所示，每个 NDN 节点都包含 3 种数据结构，分别是内容缓存库（CS, content store）、待定兴趣表（PIT, pending interest table）和转发信息表（FIB, forwarding information base）[12]。CS 用于缓存节点收到的数据分组内容，相同的内容请求可能会在路由器节点得到快速及时的响应，从而减少了内容请求对于内容源的访问次数并避免冗余流量的重复传输。PIT 用于记录已经转发出去但未被响应的请求分组的内容名及其来源的接口，PIT 可以让经过一个节点并请求具有相同内容请求分组汇聚在一个表项中，这个过程仅转发一个该请求分组，返回的数据分组按照 PIT 的指示，沿请求分组转发的路径反向返回，准确到达请求方。FIB 类似于 TCP/IP 网络中的 FIB，都是依靠路由协议生成，记录着当前节点通往内容源或内容缓存节点的下一跳接口，是节点转发请求分组的依据。

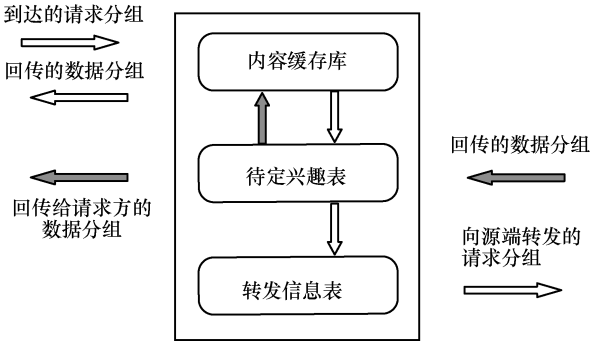


图 2　命名数据网络单个节点通信流程

因此，NDN 的通信流程可以分成 2 种情况，如图 3 所示。

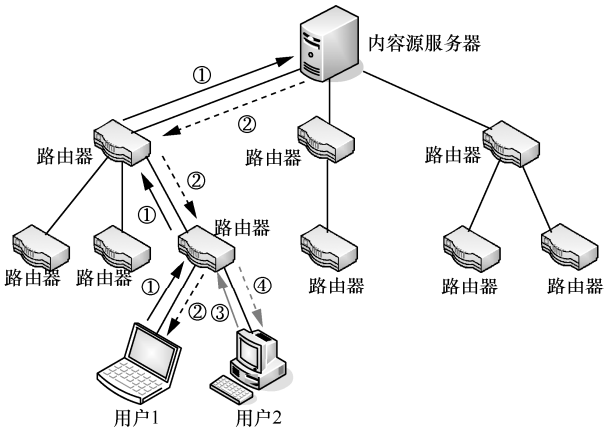


图 3　命名数据网络全网通信流程

1) 当 NDN 节点收到一个请求分组时，首先检查 CS 中是否有请求分组所需请求的内容，若有，则将内容从请求分组到来的端口转发回请求方；若没有，则检查 PIT 中是否已经记录着所请求的内容名，若已有记录，说明已经有请求相同内容的请求分组经过该节点并转发出去，此时，只需要将当前请求分组到来的端口记录到 PIT 中即可；若 PIT 中无匹配的表项，则在 PIT 中添加完整的表项并基于 FIB 和转发策略将请求分组向内容源方向进行转发。

2) 当 NDN 节点收到一个数据分组时，首先通过最长前缀匹配的方式找到匹配的 PIT，并将数据分组按照匹配表项给出的端口向请求方转发；若没有匹配的 PIT，说明当前节点以及相关的请求方不需要该数据分组中的内容，则丢弃该数据分组。每

当 NDN 节点收到并转发一个数据分组，都会将 PIT 中匹配的表项删除，同时将数据分组中的内容缓存在该节点的 CS 中。

由于 NDN 的每一个数据分组自身都携带着命名前缀和签名，内容的请求和获取与请求方、发布方的身份以及位置都没有关系，因此，通过缓存内容的方式可就近响应内容的请求，不仅可以减少请求与响应之间的时间间隔，减轻请求对内容源服务器的访问压力，同时在出现分组丢失时，可以向最近的缓存节点请求并获取内容，而不需要再次向远处的服务器请求，在多播和请求重传场景下的内容转发性能得以提升[12]。与 TCP/IP 网络中需要事先建立端到端连接的缓存机制不同，NDN 中内容的请求和获取不依赖于端到端连接的传输模式，而是一种内容分发式的查找与传输。如图 3 所示，当查找最近的缓存节点没有相应可用的缓存内容时，请求分组会最终到达内容源服务器（过程①和②）。若发现节点缓存有可用的内容时，缓存节点会就近响应请求，并将内容返回给请求方（过程③和④）。

3.3 命名数据网络优势

作为一个请求方驱动的内容分发网络，NDN 具有网内缓存机制，可以加速内容数据的同步；并且 NDN 关注的是内容本身，NDN 分组结构可以将数据安全细化到分组层面，即对每一个分组进行签名和验证，很好地细化了安全粒度并保证安全性；同时链路状态与缓存内容状态保持一致性，基于命名数据链路状态路由协议（NLSR, named-data link state routing protocol），不仅可以保证 NDN 中各节点链路状态的全网一致性，同时可以保证 NDN 各节点缓存内容状态的一致性，即运行 NLSR 的 NDN 中的任意一个 NDN 节点，通过维持一个链路状态数据库（LSDB, link state database），可以知道某个内容的内容源和内容缓存节点在网络中的位置以及如何到达这部分节点。

区块链技术作为一个去中心化的分布式数据广播通信模式，在解决其信息传输问题方面，如果采用 NDN 模型，将有以下优势。

1) NDN 的网内缓存机制可以缓解新区块全网同步在 IP 网络端到端连接产生的大量通信开销，还可以减少访问区块所在节点的网络流量，避免网络拥塞，同时加快区块同步的速度。

2) NDN 基于名字的路由和转发，在安全隐私方面相对于现在的 IP 网络是一个很大的优势，与区块链“隐藏交易各方信息，公开交易内容”的设计思想高度吻合。

3) NDN 中链路状态与缓存内容状态的一致性，可以满足区块链技术需要全网各节点备份相同的区块链数据的需求一致。同时也是去中心化的表现，符合区块链技术的设计思路。

4 基于命名数据网络的区块链信息传输架构

传统的命名数据网络是基于用户“分发”（pull）的模式来完成通信过程的，即用户会主动在网络中发起对数据对象的请求分组，再通过路由器节点的路由和转发，将该请求分组送达内容源，进而获取到用户的数据对象。然而，对于区块链技术而言，其应用场景都是基于点对点传输的实时通信，即每个通信节点主动将自己产生的数据对象“推”（push）送给对应应用场景里的所有其他通信节点。因此，如果人们基于命名数据网络来解决区块链信息传输的问题，就需要命名数据网络也支持这种用户订阅的模式，通信节点仅会将其本身产生的数据对象推送给已知的订阅用户（即应用场景中的其他点对点通信节点）。

因此，在基于命名数据网络的区块链信息传输架构中，人们仍然在兼容命名数据网络现有通信模式（即保留其支持分发服务的特征）的情况下，同时增加其支持推送服务的能力。通过构造特殊的请求分组格式，触发通信节点将其产生的数据对象推送给应用场景内的所有其他目标通信节点。

对于区块链应用场景的每个通信节点（用户终端或服务器）在命名数据网络通信环境中，如果想接收到产生数据对象的节点“推”送的数据对象，就需要所有的通信节点定期向网络中发送请求分组，这部分请求分组的类型即控制信令类型，路由建立算法如算法 1 所示，用于表达自身节点的活跃状态（继续参与被动推送和主动请求的应用场景或退出该应用场景）。如果请求分组中节点表达自身为活跃状态，则路由器中相应添加此条路由项，再转发到下一路由器重复上述过程；如果请求分组中节点表达自身为退出状态，则路由器删除相应的路由项。接收到该种请求分组的节点再继续响应一个表明已添加该节点到接收“推”送信息联系人列表或已删除该联系人的数据分组。因此，命名数据网络中的路由器就是根据节点发送的请求分组带有的信息来建立整个网络中的初始路由，便于后续通信的路由和转发。

算法 1　基于命名数据网络的区块链信息传输架构节点路由建立算法

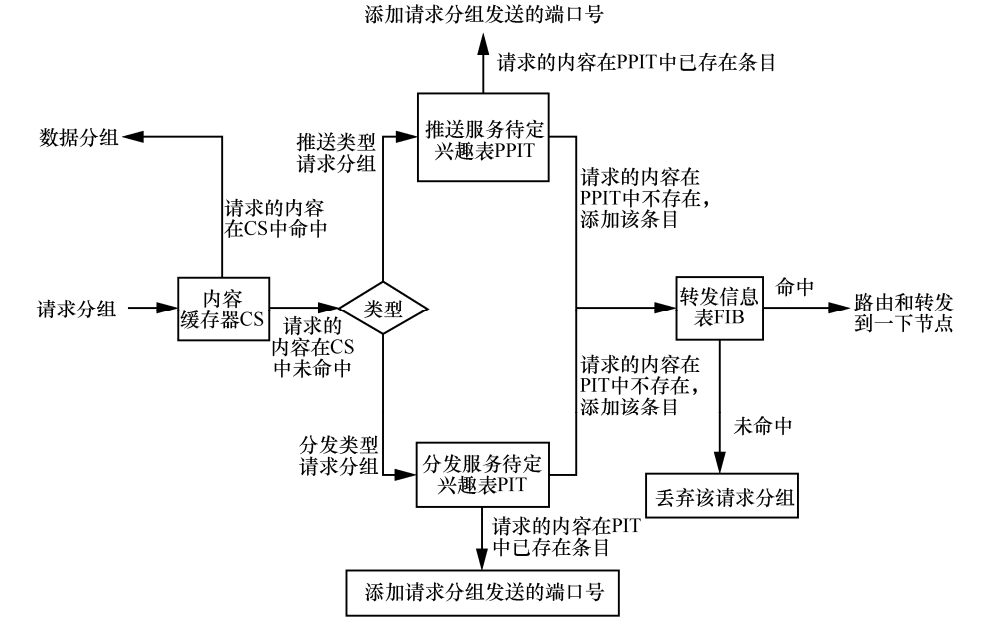
1) /*判断请求分组类型*/
　if 请求分组类型 = 控制信令类型 then
　　goto 3)
2) /*非控制信令类型请求分组处理*/
　if 请求分组类型 = 推送服务类型 then
查询 PPIT 处理
　else /*请求分组类型 = 内容分发类型*/
　查询 PIT 处理
goto 4)
3)　/* 区块链应用场景驱动节点动态路由表建立*/
　if 通信节点状态 = positive then
　　if FIB 中不存在该通信节点信息 then
　　在 FIB 中添加该通信节点名字和请求分组来的端口号
　　else /* FIB 中存在该通信节点信息*/
　　goto 5)
　else /*通信节点状态 = negative*/
　在 FIB 中删除该通信节点名字和请求分组来的端口号
　goto 5)
4) 根据 FIB 转发请求分组到下一节点
　exit
5) 控制信令请求分组转发到下一节点

在基于命名数据网络的区块链信息传输架构的设计中，将区分“推”送类型的请求服务和“分发”类型的请求服务。因此，在原有命名数据网络节点模块的原型基础上，增加推送服务待定兴趣表（PPIT），用于记录实时“推”送类型服务的请求分组信息，而待定兴趣表（PIT）仍然只负责记录非实时“分发”类业务的请求分组信息。PPIT 的功能类似于 PIT，负责指导数据分组“回传”的路径，需要在请求分组发的过程中记录下请求的“推”送内容名和数据分组回传应该经过的端口号。考虑到“推”送类型业务主动将自己产生的数据内容“推”送给应用场景中的其他通信节点的特征，为了减少交互次数，提高链路利用率并减小内容传输时延，通过“推”送方主动发送的请求分组来构造一个假的接收方发来的对该“推”送内容的请求，建立一个反向的写待定兴趣表过程，如算法 2 所示，这样不需要接收方请求就可以将内容推送过去。同时考虑到实时类业务的持续推送，避免对同一内容的后续内容块再重复发送请求分组或数据分组造成时延、体验差等问题，在数据回传的过程中，PPIT 将不会删除已完成记录条目，同时会增加记录数据分组序列号的功能。具体通信流程如图 4 所示。

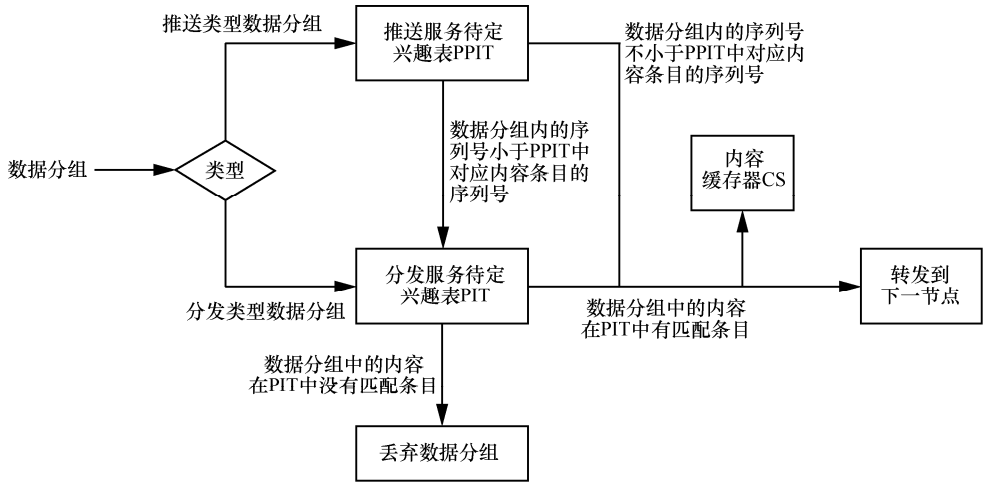
算法 2　“推”送类型业务 PPIT 建立算法

1) /*判断请求分组类型*/
　if 请求分组类型 = push 类 then
goto 2)
　else /*请求分组类型 = pull 类*/
　执行 PIT 表建立过程
　exit
2) /*推送方主动发送特殊请求分组，建立 PPIT*/
　if PPIT 中不存在该待推送内容信息 then
　　PPIT 记录推送内容名字
　　/*构造反向的写待定兴趣表过程*/
　　PPIT 记录从本节点发送出去的端口号到相应的入端口表项中
　　/*记录时间戳，便于区分同一数据内容的不同的内容块*/
　　PPIT 记录数据对象序列号
　else /* PPIT 中存在该待推送内容信息，判断该请求分组出端口号和入端口号是否匹配*/
　　if out port = in port then
　　exit
　　else
　　记录出端口号在入端口表项中

当有请求分组到达时，首先在内容缓存器 CS 中查找是否已经缓存该内容，若有则直接返回该内容数据分组，否则判定该请求分组的类型。若为区块链应用（即推送类型）请求分组，则查询推送服务待定兴趣表 PPIT，如果该请求内容的名字已经在 PPIT 中存在，则相应地进行写反向待定兴趣表过程；如果该请求内容的名字在 PPIT 中不存在，则相应地添加该请求分组全部信息条目（内容名字、写反向待定兴趣表入端口表项端口号、推送内容序列号），再通过路由信息表进行路由转发到下一节点。如果判定该请求分组类型为分发类服务请求分组，则按照常规的待定兴趣表 PIT 操作进行处理。而在数据分组处理的过程中，首先判断数据分组的类型，如果是分发类业务的数据分组，则按照常规的命名数据网络流程处理；如果是区块链业务的数据分组，



(a) 请求分组



(b) 数据分组

图 4　基于命名数据网络的区块链信息传输通信流程

则在相应的 PPIT 中进行查询，若数据分组中的内容序列号不小于 PPIT 中对应条目的序列号，则按照 PPIT 中记录的端口号进行转发，表明该数据分组中包含的是其他用户实时请求的当前最新产生的业务数据或者相应业务数据后续内容块的持续推送；若数据分组中的内容序列号小于 PPIT 中对应条目的序列号，尽管该数据分组也是推送类型的，但是却不是实时业务，则通过 PIT 进行下一步的处理。

尽管这里增加了新的表结构，但是通过反向写待定兴趣表的过程，使支持推送类型业务的 NDN 仍然只需发送一次请求就可以对应获得一个数据分组，这意味着建立新表本身不会带来附加的分组开销。事实上，引入新表增加的是路由器的处理能力，要求路由器在收到请求分组时，首先分析分组类型，一方面基于现有硬件的发展能力，另一方面基于 NDN 本身的以数据命名的思想和方式，所以这并不会给路由器的处理过程增加太多的复杂度，就能实现新的业务支撑能力。

5　基于命名数据网络的区块链信息传输实例/应用场景

正如第 2 节所述，随着区块链技术的不断发展，其衍生出多种形态，包括公有链、私有链、联盟链和侧链。结合区块链技术目前主要的应用趋势，本

节主要以公有链的形式为代表，详细介绍虚拟货币这种基于区块链技术的应用场景是如何在本文提出的基于命名数据网络的区块链信息传输架构之上实现通信和交易过程的。

虚拟货币作为一个典型的公有链形式，是区块链技术最早且最有代表性的应用场景。在基于命名数据网络的区块链信息传输架构之上部署的虚拟货币应用场景如图 5 所示。当用户 A 使用虚拟货币向商家 Z 付款完成一笔交易时，首先 A 发送正常的请求分组给 Z 获取 Z 的收款地址（该地址用于存放虚拟货币），Z 收到该请求分组后创建一个新地址用于接收 A 的款项，并将该地址通过数据分组回传给 A。A 收到 Z 的数据分组后，在自己的“钱包”（包含多个虚拟货币地址）中选择付款地址，并用相应的私钥（每个地址对应一个私钥）加密该笔交易申请。这里假定参与虚拟货币交易的矿工为图 5 中所示的矿工 C~矿工 G，用户 A 已经添加矿工 C~矿工 G 为自己的联系人列表。此时用户 A 发送 push 类型请求分组给所有联系人列表成员（包括所有的矿工和商家 Z），网络中的路由器节点进行反向写 PPIT 过程，构造一种所有矿工和商家 Z 向用户 A 共同发起对该笔交易申请的请求分组的“假象”，然后用户 A 将该笔交易申请以 push 类型数据分组的形式发送出去，网络中的路由器节点根据 PPIT 中记录的信息转发该数据分组到所有虚拟货币应用场景中的通信节点。矿工 C~矿工 G 收到数据分组后，使用相应的公钥验证该笔交易的合法性，将一段时间内的交易数据打包成一个新的交易块，计算新的散列值，从而形成新的账本，最先计算出符合规则的散列值的矿工（比如矿工 D），会获得虚拟货币奖励，包含在这个新的区块中，矿工 D 同样发送 push 类型请求分组给所有其他矿工，建立 PPIT 之后，D 再发送它计算好的区块以 push 类型数据分组形式给其他矿工，以记录下这笔交易，保证交易生效和账本不可篡改。

在这个过程中，账本中每个区块都会在网络路由器节点中缓存下来，便于后续新加入虚拟货币应用中的任何人来获取区块，存储完整的账本或去加入验证交易的矿工行列，减少用户获取数据的时延并且更好地保证用户体验。同时，基于命名数据网络特有的路由器 PIT 和本文提出的 PPIT 结构和设计，请求分组具有聚合的特征，避免了数据分组大量的重复传输，缓解了网络的压力，更适合未来内容量和数据传输量大幅度增加的场景。

6　仿真结果与分析

命名数据网络基于名字路由、路由器 PIT 聚合特征、路由器缓存能力的设计原理，能够天然支持多播和广播，相比 IP 网络基于端到端的连接通信设

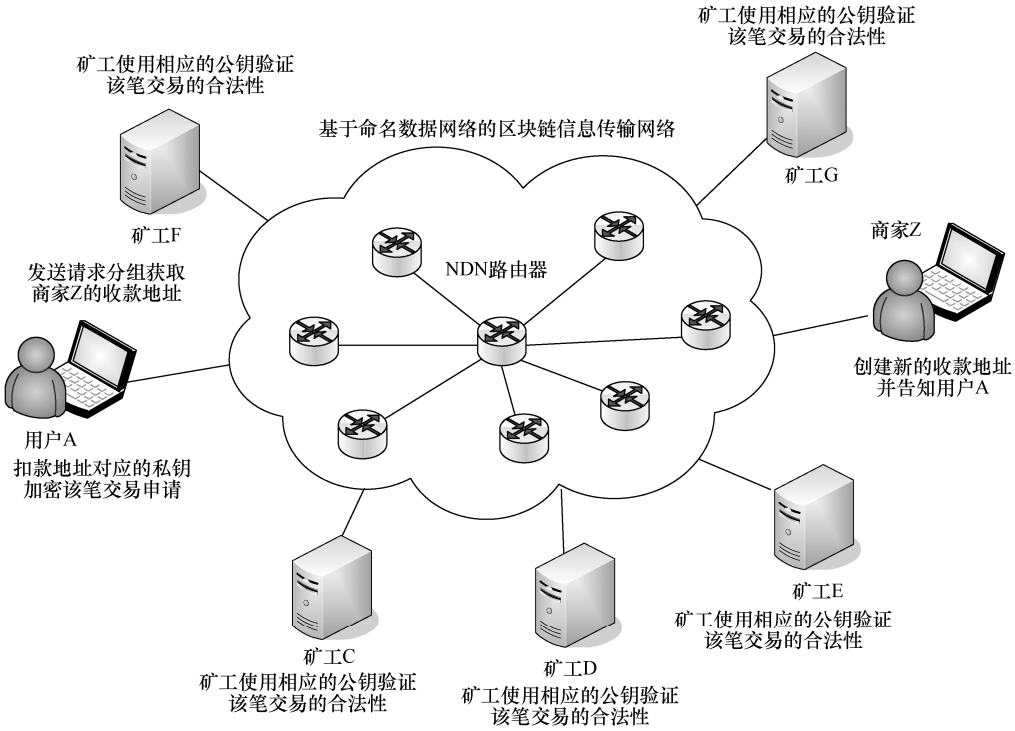


图 5　在基于命名数据网络的区块链信息传输架构中部署虚拟货币应用场景

计相比，可以在一定程度上减少网络流量的冗余、拥塞和传输的开销，优化网络性能。这里采用如图 5 所示的应用场景，采用一个典型的星型拓扑连接一个用户、一个商家和 5 个矿工，在规定的 7×10^4 s 时间内由用户 A 向商家 Z 发起 100 笔交易，5 个矿工配有相同且充足的计算和存储能力，假定每个区块数据分组的固定大小为 1 MB。

如图 6 所示，随着时间的变化，交易不断发生，每发生一笔交易，由矿工进行验证和记账，生成区块，一般一个区块的生成平均大概在 10~15 min 左右。对于不同的网络而言，由于通信模式的不同，区块链信息在传输过程中会有不同的通信开销，如图 7 所示，由于命名数据网络的设计充分支持多播，基于命名数据网络的区块链信息传输相比基于 IP 网络的区块链信息传输可以降低网内流量达到 17%左右。

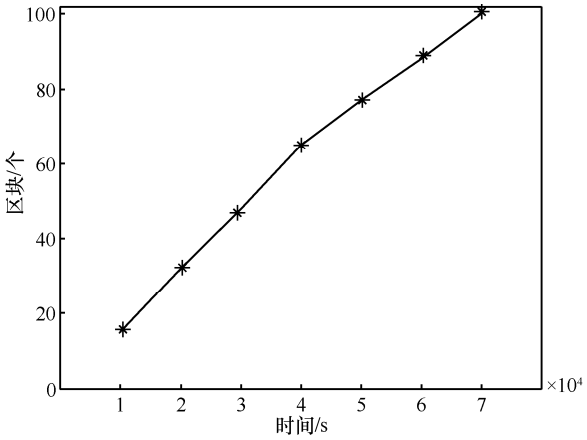


图 6　规定时间内形成区块链的区块数目变化

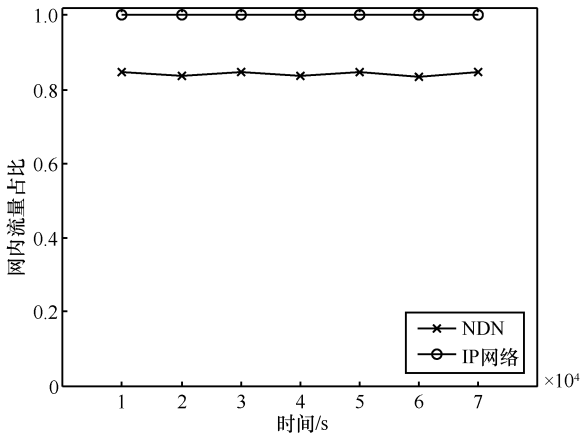


图 7　形成区块链过程中网络中流量占比统计结果

7　未来网络技术与区块链技术研究展望

综上所述，本文提出的改进的命名数据网络模式在解决区块链信息传输问题上有明显优势，源端可以主动推送数据内容给所有的接收方，并且利用 NDN 聚合的特性，一份数据可以通过分叉的方式发送给所有的接收方，数据发送失败或再次被请求都可能在路由器中得到命中，可以很好地支撑基于区块链技术的各类交易记账型应用，从通信的角度看，保证这些业务具有更好的实时性。尽管命名数据网络对于区块链技术的通信问题可以提供很好的解决方案，但是仍然希望可以使更多有前景的未来网络技术与区块链技术进行融合，让未来网络技术和区块链技术更好地服务彼此，进一步推广应用。

软件定义网络是目前应用最为广泛的未来网络技术之一，通过控制平面和数据平面的分离，能够通过中央控制器以全局的视角智能化地管理整个网络。而在区块链的分类中，包括公有链、联盟链和私有链等，它们各自具有不同的去中心化程度，企业级的联盟链和用户级的私有链算是部分去中心化的模式，少数级别较高的用户系统甚至具有修改或者读取其他普通用户系统的能力。例如，在智能电网的应用中，普通用户不仅可以消耗电能，也可以产生电能并把自产的电能卖给其他用户，这些普通用户的交易可以通过区块链技术来完成共享账本的建立，同时在电网级的私有链中需要有更高级别的管理系统，结合软件定义网络集中管控的能力，可以实现对整个电网进行全局实时监管。因此，在未来的研究中，可以从区块链技术（私有链）和软件定义网络结合的角度去考虑如何加速智能业务的快速部署和实现。

随着互联网规模的不断壮大及其使用的普及化，复杂多样的信息内容源源不断地产生，因此，“大数据”这一概念是在互联网发展到一定的阶段自然呈现出来的现象和特征。而如果想让这些大数据产生出更多真实的价值，就涉及方方面面诸如隐私安全权益等的问题。为了让大数据发挥其更大的价值，未来可以利用区块链这种具有高可信任性、安全性和不可篡改性的特征来解决这一问题。例如区块链技术中采用非对称加密技术和散列加密算法能够保证数据私密性，可以杜绝数据共享中的信息安全问题，大数据在被利用的同时又不会暴露数据来源的任何个人信息。同时区块链技术作为基于全网共识的特殊数据库能够保证数据的不可篡改。如此，在未来的研究中，可以从区块链技术和大数

据技术结合的角度展开研究，让大数据的角色更加活跃起来。

8　结束语

本文简要综述了区块链技术和命名数据网络的原理并详细分析了各自的特征、优势以及应用前景。基于充分的研究并针对区块链技术信息传输问题，提出了一种基于命名数据网络的区块链信息传输的架构，改进了原有的仅支持用户“分发”模式的命名数据网络模型，设计了新的增加支持源端“推”送模式的节点模型和特殊的写表项过程，使区块链技术在命名数据网络上的部署达到了更好的契合度。同时，就虚拟货币场景，给出了完整的基于本文提出架构的应用场景实例，有助于更好地理解本架构的实施原理，并且通过仿真验证本方案的性能优势。最后，就未来网络技术与区块链技术彼此推动的一些领域给出一定的研究展望，并将进一步展开研究工作。

参考文献：

[1] SWAN M. Blockchain: blueprint for a new economy[M]. USA: O Reilly Media Inc, 2015.

[2] SCHNEIDER J, BLOSTEIN A, LEE B, et al. Blockchain: putting theory into practice[R]. USA: the Goldman Sachs Group Inc, 2016.

[3] 林小驰, 胡叶倩雯. 关于区块链技术的研究综述[J]. 金融市场研究, 2016, 45(2): 97-109.
LIN X C, HU Y Q W. A summary of blockchain technology[J]. Financial Market Research, 2016, 45(2): 97-109.

[4] 杨辉, 张杰. 传统宽带网络面临挑战, 区块链技术为其转型升级[J]. 通信世界, 2016(21): 48-50.
YANG H, ZHANG J. Traditional broadband networks are facing challenges, using blockchain technology for transformation and upgrading[J]. Communication World, 2016(21): 48-50.

[5] 唐文剑. 区块链将如何重新定义世界[M]. 北京: 机械工业出版社, 2016.
TANG W J. How will blockchain redefine the world[M]. Beijing: China Machine Press, 2016.

[6] TEEMU K, MOHIT C, BYUNG-GON C, et al. A data-oriented (and beyond) network architecture[C]//The 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM’07). 2007: 181-192.

[7] FOTIOUS N, TROSSEN D, POLYZOS G. Illustrating a publish-subscribe Internet architecture[J]. Journal on Telecommunication Systems, 2012, 51(4): 233-245.

[8] DOMINGUEZ A M, NOVO O, WONG W, et al. Publish/subscribe communication mechanisms over PSIRP[C]//The 2011 7th International Conference on Next Generation Web Services Practices (NWeSP). 2011: 268-273.

[9] HOQUE A K M M, AMIN S O, ALYYAN A, et al. NLSR: named-data link state routing protocol[C]//The 3rd ACM SIGCOMM Workshop on Information-Centric Networking (ICN’13). 2013: 15-20.

[10] AFANASYEV A, SHI J, ZHANG B, et al. NFD developer’s guide[R]. Technical Report NDN-0021, NDN, 2015.

[11] MASTORAKIS S, AFANASYEV A, ZHANG L. On the evolution of ndnSIM: an open-source simulator for NDN experimentation[J]. ACM SIGCOMM Computer Communication Review, 2017, 47(3): 19-33.

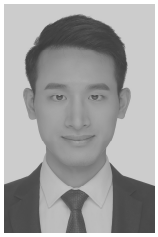
[12] ZHANG L, AFANASYYEV A, BURKE J, et al. Named data networking[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66-73.

[作者简介]

刘江（1983-），男，河南郑州人，博士，北京邮电大学副教授，主要研究方向为网络体系架构、网络虚拟化、软件定义网络、信息中心网络等。

霍如（1988-），女，黑龙江哈尔滨人，博士，北京工业大学讲师，主要研究方向为计算机网络、信息中心网络、网络缓存策略与算法等。

李诚成（1989-），男，河北石家庄人，北京邮电大学博士生，主要研究方向为软件定义网络、信息中心网络、5G 网络架构等。



邹贵今（1993-），男，广东揭西人，北京邮电大学硕士生，主要研究方向为信息中心网络、计算机网络。

黄韬（1980-），男，重庆人，博士，北京邮电大学教授，主要研究方向为路由与交换、软件定义网络、内容分发网络等。

刘韵洁（1943-），男，山东烟台人，中国工程院院士，北京邮电大学教授，主要研究方向为未来网络技术、网络体系架构、网络融合与演进等。