



基于NDN的区块链网络服务质量保障方法

尚佳佳¹, 霍如^{2,3}, 耿丽萍⁴, 汪硕^{1,3}, 黄韬^{1,3}

(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.北京工业大学信息学部,北京 100124;
3.紫金山实验室,南京 211111; 4.中国人民解放军61932部队,北京 100088)

摘要:针对传统区块链网络难以满足不同应用场景差异化服务质量(QoS)需求的问题,提出一种基于命名数据网络的区块链网络QoS保障方法。从实时性角度对交易和区块进行分类,为交易和区块设计新的命名空间。为不同类型的区块链数据创建各自的数据传播结构,以缓解流量的集中化程度。针对不同应用场景对实时性的要求,采用差异化路由机制对交易和区块进行排队转发。实验结果表明,该方法能够有效提高区块链网络的信息传输效率,减少网络中的冗余流量,其网内流量相比基于TCP的区块链网络约下降24%。

关键词:区块链;命名数据网络;数据传播;服务质量;差异化服务

开放科学(资源服务)标志码(OSID):



中文引用格式:尚佳佳,霍如,耿丽萍,等.基于NDN的区块链网络服务质量保障方法[J].计算机工程,2021,47(12):40-46,53.

英文引用格式:SHANG J J, HUO R, GENG L P, et al. Quality of service assurance method for blockchain network based on NDN[J]. Computer Engineering, 2021, 47(12): 40-46, 53.

Quality of Service Assurance Method for Blockchain Network Based on NDN

SHANG Jiajia¹, HUO Ru^{2,3}, GENG Liping⁴, WANG Shuo^{1,3}, HUANG Tao^{1,3}

(1.State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China; 2.Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China; 3.Purple Mountain Laboratories, Nanjing 211111, China; 4.Unit 61932 of the Chinese People's Liberation Army, Beijing 100088, China)

[Abstract] The traditional blockchain networks cannot meet the differentiated Quality of Service (QoS) demands in different application scenarios. To solve this problem, a QoS assurance method for blockchain network based on Named Data Networking (NDN) is proposed. Transactions and blocks are categorized according to real-time requirements, and a new namespace is designed for them. Then different data propagation structures are created for different types of blockchain data to reduce the concentration of traffic. A differentiated routing mechanism is adopted to queue and forward transactions and blocks according to the different real-time performance requirements in different application scenarios. The experimental results show that the proposed method can significantly improve the information transmission efficiency of blockchain network, and reduce the redundant traffic in the network. It can also decrease the intra-network traffic by about 24% compared with TCP-based blockchain networks.

[Key words] blockchain; Named Data Networking (NDN); data transmission; Quality of Service (QoS); differentiated services

DOI:10.19678/j.issn.1000-3428.0061950

0 概述

传统的区块链技术大多在P2P(Peer-to-Peer)网络中基于TCP网络架构^[1]并通过应用层多播实现数据传输,而且不同终端节点对于同一个数据内容的

请求相互独立,导致网络中存在大量冗余流量以及较高的数据传输时延^[2]。命名数据网络(Named Data Networking, NDN)将IP网络沙漏模型的细腰部分更换为内容名称,基于内容名称进行数据传输,其关注点在于内容本身,和区块链的设计思想(即隐藏交易

基金项目:2019年工业互联网创新发展工程基金项目“创新型工业互联网标识解析系统”。

作者简介:尚佳佳(1995—),女,硕士研究生,主研方向为区块链、命名数据网络、路由策略;霍如,讲师、博士;耿丽萍,工程师;汪硕,讲师、博士;黄韬,教授、博士。

收稿日期:2021-06-18 修回日期:2021-08-20 E-mail:shangjiajia_bupt@163.com

各方信息,公开透明交易内容)相符合。区块链技术已广泛应用于金融、智慧医疗、智能电网等场景;资金跨境支付结算^[3]需要多个中间机构合作构建汇款通道以完成支付结算,其中涉及多个参与方,该过程需要保障支付结算的安全性和隐私性^[4];金融行业对交易实时性要求较高,需要实现较低的时延^[5];智慧城市关注居民、设施等各类数据的收集、分析和处理,要求保障数据安全和用户隐私。在实际应用中,需要针对不同场景差异化的服务质量(Quality of Service, QoS)需求来设计有针对性的解决方案。

本文提出一种基于NDN的区块链网络QoS保障方法。为满足实时性要求,将交易和区块分为时延较敏感和时延较不敏感2种类型,设计新的命名空间,为不同类型的区块链数据创建各自的数据传播结构。在此基础上,针对不同应用场景对实时性和QoS的不同要求,采用差异化路由机制对交易和区块分别进行排队转发。

1 区块链和命名数据网络

区块链中的各节点具有分布式、对等的特性,因此,一般采用P2P网络来组织负责数据验证和记账的节点^[6]。P2P网络中的每个节点地位均等,不存在任何中心化的节点或者特殊节点和结构,每个节点都可以进行交易验证、交易传播、区块验证、区块传播等。

区块链节点在网络中进行交易(区块)的分发和接收,并且通过一系列的验证机制^[6]验证交易(区块)的有效性。区块链系统的交易(区块)传播机制主要包括以下步骤:

- 1) 区块链节点将新生成的交易广播给邻居节点,邻居节点收到后继续广播。

- 2) 每个节点将在网络中广播的交易收集到区块中,并且基于自身算力寻找一个难度与自身算力相匹配的工作量证明^[7],算力较弱的节点会相互合作建立矿池,汇聚算力以共同解决一个难题,在找到工作量证明之后即全网广播该区块。

- 3) 网络中的其他节点在收到区块后对区块中包含的交易进行验证,当且仅当区块中包含的所有交易都是有效的并且之前没有存在过,才认为该区块有效。

- 4) 在验证区块有效之后,其他节点接受该区块并在该区块末尾产生新块延长链。

NDN基于数据内容名称进行路由转发,每个数据分组对应唯一的内容名称^[3]。节点若要接收特定的内容,需要主动向网络中发送对该内容的兴趣请求,即“订阅”该内容,内容所有者或者缓存有该内容的路由器节点接收到兴趣请求后^[8],则将该内容按照请求分组路由方向的反方向发送给请求者。

NDN分组类型具体如下:

- 1) 请求分组(兴趣包)。请求分组为内容请求者向内容所有者发送的用于请求特定内容的分组^[9]。请求分组模型包含内容名、选择器和随机数。

- 2) 数据分组(数据包)。数据分组为内容源或内容缓存者响应内容请求者的请求向请求者返回的内容,数据传输路径按照请求分组传输路径的反方向进行^[10]。数据分组模型包含内容名、签名、署名信息和数据内容。

NDN数据结构具体如下:

- 1) 内容存储(Content Store, CS)。CS结构由数据内容名称和数据2个条目构成,其缓存节点收到的数据分组内容^[11]。网络中存在大量关于相同数据内容的请求,CS的存在能让后续请求相同内容的节点得到快速及时的响应。

- 2) 待定兴趣表(Pending Interest Table, PIT)。PIT记录已经转发出去但没有收到响应的请求分组的内容名称及其到来的路由器接口^[12],将经过同一个路由器节点并请求相同内容的请求分组汇聚在一个表项中,对同一内容的请求,仅转发一次对该内容的请求分组,无需重复转发。在数据分组回传过程中,PIT表中有该内容名称的路由器将该内容缓存在CS中^[13],后续其他节点请求该内容时直接由拥有该内容的邻近路由器返回即可,无需再次向内容生产者请求。

- 3) 转发信息库(Forwarding Information Base, FIB)。FIB包含名称前缀和接口列表2个条目,其和TCP/IP网络体系架构中的路由表类似,依靠路由协议生成^[14],记录从当前路由器节点通往内容生成者或内容缓存节点的路径上的下一跳接口。

然而,区块链基于内容所有者主动推送的“推”模式与NDN基于内容请求者主动请求的“拉”模式互不兼容。文献[7]在NDN上启动区块链应用程序,将交易包含在兴趣包中支持交易的实时广播,使用“订阅-推送”来支持区块的广播,矿工执行订阅操作,区块生成之后所有订阅的矿工就会收到该区块。文献[8]通过“发布-订阅”模式兼容区块链,采用分层的命名空间实现流量隔离。文献[9]引入分层命名机制并实现区块的批量同步。以上方法解决了区块链和NDN的兼容问题,并针对数据同步等需求提出解决方案,但是没有考虑到不同应用场景差异化的QoS需求。为满足应用场景的实时性要求,本文对传统的命名空间进行改进,在NDN中路由转发时即可基于数据名称中的实时性要求标识采用差异化的路由策略;通过为每种类型的数据创建专属的数据传播结构来降低流量集中化程度,使得流量均匀地分布于网络各处,提高网络资源的利用率;采用差异化的路由机制对区块链各类型数据分别进行路由转发,从而满足不同应用场景差异化的QoS需求。

2 网络服务质量保障方法

现有在NDN上部署区块链的方法仅利用NDN的一些特性对区块链进行局部优化(如重新设计命名空间),区块链与NDN的融合程度还有待提高。此外,差异化服务的思想在TCP/IP体系下已经非常成熟^[15],且表现出较好的性能。随着NDN技术的发展,当区块链建立在NDN上时,也应具备更加精细的差异化服务,而这一方面目前较少有针对性的研究。因此,本文提出一种能够提供差异化服务的解决方案,以完善区块链业务。

针对不同应用场景提供差异化的QoS保障可以发挥以下作用:

1) 优化网络资源分配。NDN基础设施通常带宽有限^[16],为区块链建立专用的NDN网络并不能在实际中得到应用,因此,有必要为其在网络层面提供差异化服务,从而缓解区块链业务给NDN设备带来的处理压力。

2) 提高区块链的性能。基于TCP的区块链难以提供对多播的内置支持^[17],导致在同质节点之间建立连接需要较长的同步时间,而且交易的验证、分发等会导致大量的数据开销,极大地限制了区块链的性能,而差异化服务可以在一定程度上打破这种限制。

3) 提高安全性和可拓展性。区块链业务通常对实时性有不同的要求^[18],优先保证部分时延较敏感的业务可以提升区块链整体的安全性、稳定性和可扩展性。

基于以上分析,本文提出一种基于NDN的区块链差异化QoS保障机制,其结构如图1所示。在网络层为不同类别的流量创建数据传播结构使得流量均匀地分布于网络各处^[11],对支撑的业务进行更细粒度的划分,主要从实时性要求角度将交易和区块进行划分,对这些交易和区块采取排队转发的路由机制,以满足不同应用场景差异化的QoS需求。

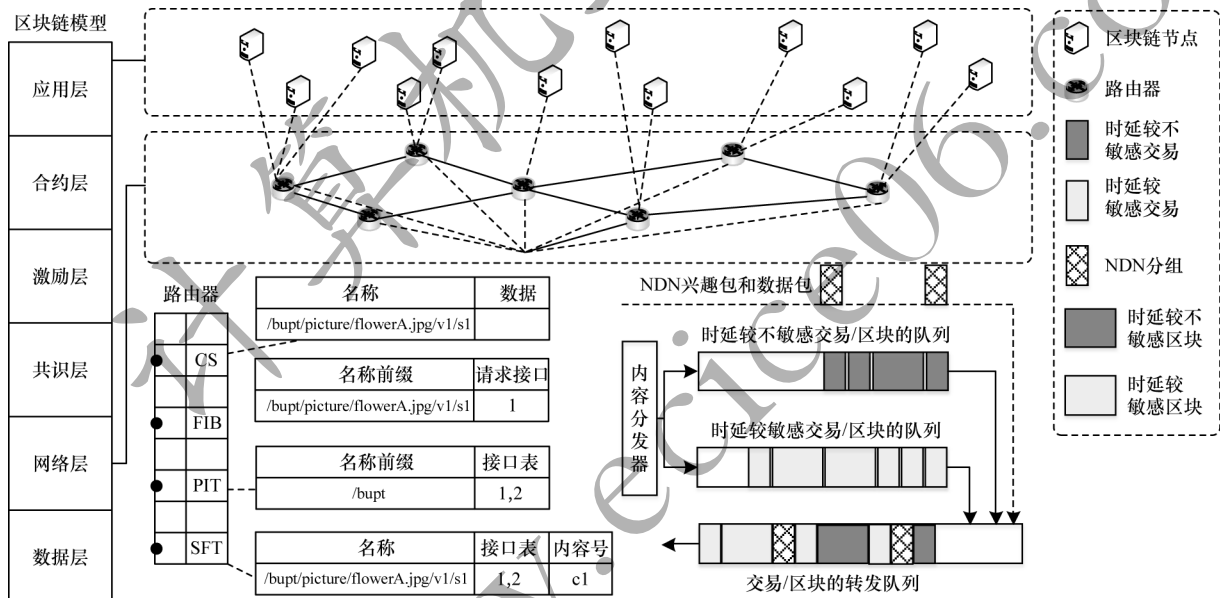


图1 QoS保障机制结构示意图

Fig.1 Structure diagram of QoS assurance mechanism

3 差异化服务质量保障方法设计与实现

本文差异化QoS保障方法首先从实时性要求角度设计分层的命名空间;其次为不同类型的交易或者区块创建数据传播结构,使网络中的流量尽可能分散在网络各处;最后设计一种差异化的路由排队机制以及兼容NDN和区块链不同模式的信息传输机制。

3.1 命名空间

NDN中基于内容名称进行数据内容路由,本文在区块链交易和区块的命名中添加“差异化服务”字段来区分类别。数据在网络中路由时基于各自的数

据传播结构,在检索时基于交易名称或者区块名称,同时路由器根据数据名称识别服务类型。因此,为满足路由、检索和服务类型识别这3个需求,数据的名称需要包括以下3个部分:

1) 类别标识符(Category Identifier, CID)。CID <Category Name>用来标识不同的数据传播结构,每种类型的交易或区块在对应的数据传播结构上传播,例如, Learning类型的交易或区块都可以在CID为 Learning的数据传播结构上分发。

2) 服务标识符(Service Identifier, SID)。本文主要从服务的实时性要求角度(即时延敏感角度)对

QoS需求进行划分,因此,SID的取值有时延较敏感(Delay Sensitive, DS)和时延较不敏感(Delay Less Sensitive, DLS)2种。路由器根据数据内容名称中的SID字段区分识别数据内容的实时性要求,然后进行差异化的路由处理。

3)检索标识符(Retrieval Identifier, RID)。考虑到在同一个数据传播结构上传播的可能是交易也可能是区块,因此,在命名中添加区分字段<T>和分别用来标识交易和区块,规定RID为<T|Transaction Name>或者<B|Block Name>。

因此,本文数据内容按照<CID|SID|RID>结构命名,例如,<Learning|DS|T|math>表示Learning类型对时延较敏感的交易math,并且所有Learning类型的交易或者区块在CID为Learning的数据传播结构上传播。

3.2 DDPT创建

大多数区块链网络都是基于P2P网络的应用层多播而实现的^[19],即节点之间直接在逻辑拓扑上建立连接,缺乏对基础网络物理拓扑的考虑,导致上层流量与底层物理网络拓扑之间不匹配^[12]。此外,传统的路由方式过多地依赖于志愿节点或性能较好的若干个节点^[20],导致网络中大量的流量集中在网络中的少部分区域。为解决以上2个问题,本文在网络层创建分布式数据传播树(Distributed Data Propagation Tree, DDPT),使流量均匀分散在网络中各处,降低对性能较好的若干个节点或者志愿节点的依赖程度,即降低中心化程度。DDPT的创建流程如图2所示。

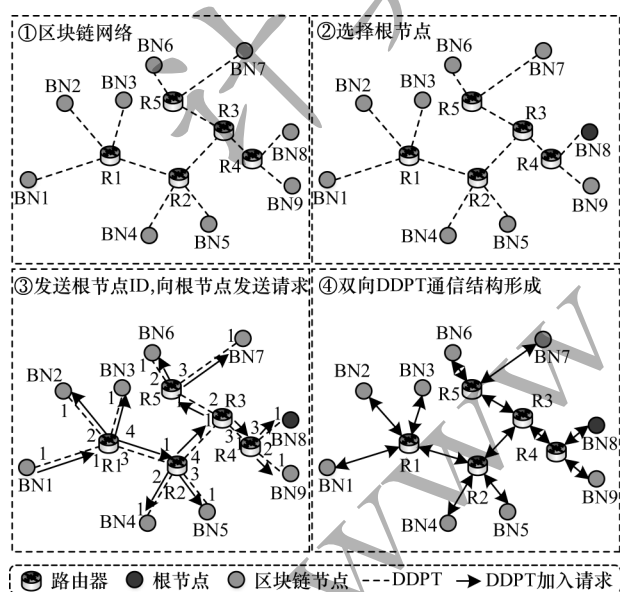


图2 DDPT的创建流程

Fig.2 The creation procedure of DDPT

DDPT创建具体步骤如下:

1)选择根节点。假设高性能区块链节点(High Performance Blockchain Node, HPBN)在网络中近似均匀分布,在由所有HPBN构成的候选子集中,选择与已有根节点(Root Node, RN)欧式距离最远的HPBN作为本次构建的DDPT的RN。

2)发送根节点ID。在选出RN之后,由发起本次DDPT构建的区块链节点(Blockchain Node, BN)向网络中的其他节点发送RN的ID。

3)请求加入DDPT。网络中其他节点在收到RN的ID之后,向RN发起加入DDPT的请求,RN在收到节点的请求之后向节点返回确认消息,DDPT创建成功。

3.3 差异化路由机制

本文从实时性要求角度对交易进行分类,将其分为时延较敏感和时延较不敏感2种类型。区块链节点自行决定收集哪种类型的交易,对不同类型的交易进行处理可以获得不同的奖励^[21]。节点收集时延较敏感交易形成时延较敏感区块,收集时延较不敏感交易形成时延较不敏感区块。NDN路由器识别交易和区块的名称,根据名称中的<SID>字段识别服务类型。

差异化路由策略需要从2个角度进行分组的判别:一是路由器节点区分收到的分组是区块链分组还是常规NDN分组;二是区分区块链类型分组的实时性要求。如图1所示,交易或区块由生成者生成命名之后发送到网络中,路由器节点收到交易或区块后,内容分发器根据内容名称中SID字段标识的实时性要求,将到达的区块分为两队,一队为时延较敏感交易/区块,另一队为时延较不敏感交易/区块,在队内按照到达的先后次序排队,NDN常规的请求分组和数据分组不参与排队。在转发时根据不同应用场景对实时性的不同需求设定不同的转发队列比例,NDN常规的请求分组和数据分组正常进入转发队列排队等待转发^[3]。在每个路由器处都执行差异化业务排队机制,以满足各类业务不同的QoS需求。基于NDN的区块链差异化路由建立算法描述如算法1所示。

算法1 基于NDN的区块链差异化路由建立算法

```

1.//判断分组类型
if 分组类型=NDN 常规分组类型 then
    转入步骤3
2.//分组类型为区块链类型分组
if 分组类型=时延较敏感分组 then
    加入时延较敏感队列
else//分组类型为时延较不敏感分组
    加入时延较不敏感队列
3.分组正常进入转发队列
4.//根据 a:b 进入转发队列, a>b 且 k 不为 0
   ak 个时延较敏感分组进入转发队列;
   bk 个时延较不敏感分组进入转发队列;
5.转发队列向下一个节点转发
  
```

3.4 信息传输机制

为兼容NDN与区块链不同的通信模式,本文在NDN基础上增加订阅推送表(Subscribe Forward Table, SFT),实时记录“推送”类型服务,即与区块链

相关的分组信息。SFT包含的信息条目包括内容名称、数据分组转发端口号、数据内容序列号。为了适配区块链基于内容生成者主动向网络中“推送”数据内容的模式,NDN网络架构中内容生成者主动向网

络中发送一个对于自己所产生内容的兴趣请求。SFT在“推送”类型请求分组分发的过程中将数据内容名和回传的数据分组经过的端口号记录在SFT表相应的条目中。信息传输流程如图3所示。

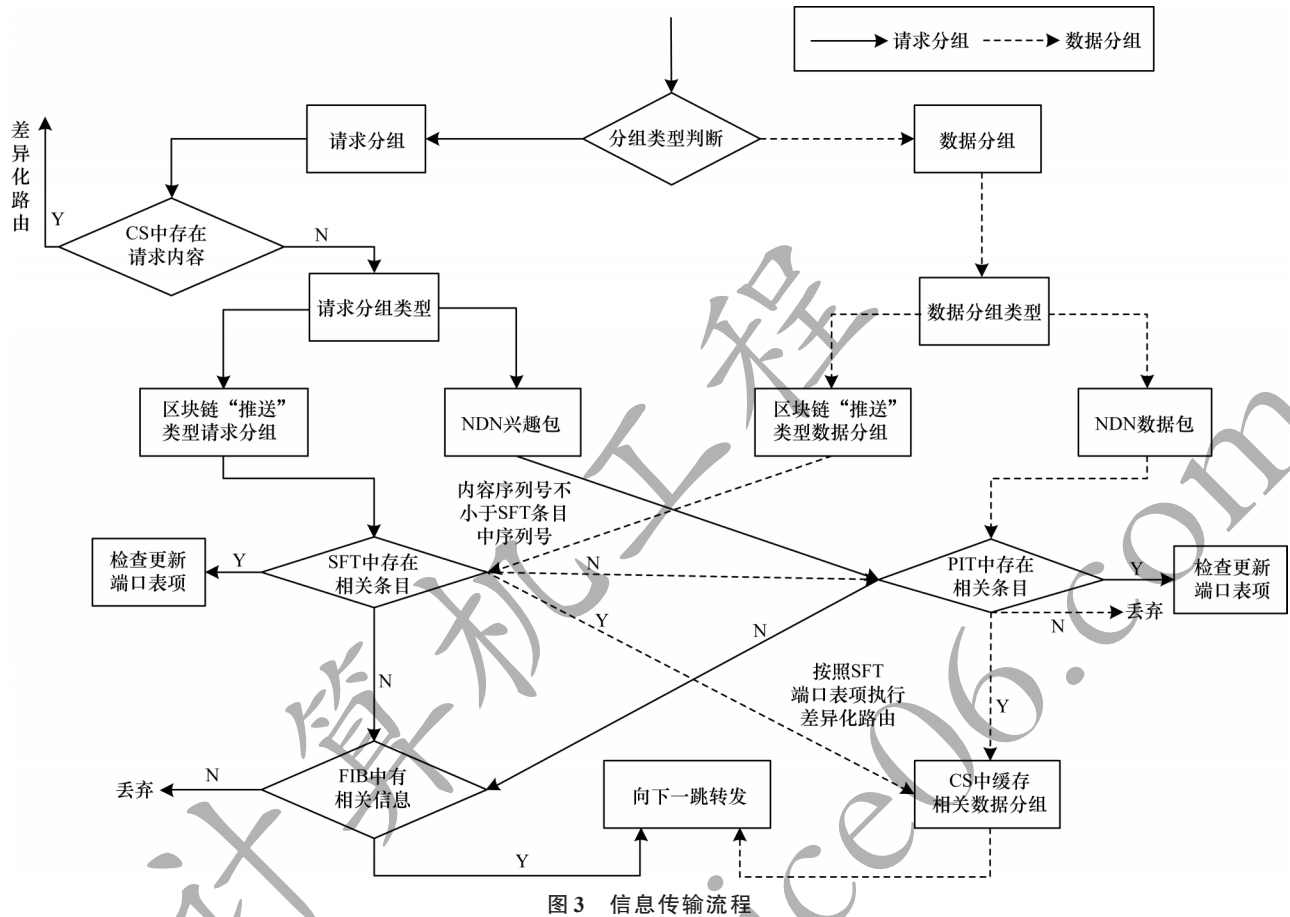


图3 信息传输流程

Fig.3 Information transmission procedure

信息传输具体步骤如下:

1)建立初始路由。所有区块链节点定期向网络中发送表达节点活跃状态的请求分组,路由器节点在收到该分组后,如果节点表达自身为“活跃”状态,则在FIB表中添加相关信息;如果节点表达自身为“退出”状态,则在FIB表中删除相关信息。路由器向其他路由器节点继续转发该请求分组,以完成初始路由的建立和状态更新。

2)建立SFT表项。数据内容生成者主动向网络中发送对自身所产生数据内容的请求分组,路由器节点在收到该请求分组后,首先判断CS中是否有相关内容,有则直接返回,没有则判定请求分组类型:若判定是区块链类型的“推送”请求分组,在SFT中查询是否有该内容的名称,若没有则在表项中添加全部信息,若有则更新SFT表中与该内容相关的接口和内容序列号信息;若判定是NDN类型的请求分组,则交由PIT表进行后续处理。

3)数据分组回传。路由器节点在收到数据分组后,首先判断数据分组类型,如果判定是区块链“推送”类型数据分组^[22],则交由SFT表,若数据分组的

内容序列号大于等于SFT中对应条目记录的内容序列号,则在内容序列号条目中添加新的序列号,按照SFT中记录的端口号转发,并且将内容缓存在CS中,若数据分组的内容序列号小于SFT中对应条目的序列号,则交由PIT表进一步处理;若判定是NDN常规数据分组,则交由PIT表进行进一步处理。

基于NDN的区块链分组通信算法描述如算法2所示。

算法2 基于NDN的区块链分组通信算法

```

1.//判断分组类型
if 分组类型=请求分组类型 then
if CS中存在请求内容 then
转入算法1
else//判断请求分组类型
转入步骤2
else//分组类型=数据分组
转入步骤3
2.//判断请求分组类型
if 请求分组=区块链请求分组 then
//查询SFT表
转入步骤4
else//查询PIT表
转入步骤5
  
```

```
3.//判断数据分组类型
if 数据分组=区块链数据分组 then
//查询 SFT 表
转入步骤 4
else//查询 PIT 表
转入步骤 5
4.//查询 SFT 表
if SFT 表中存在相关条目 then
if 分组类型=请求分组 then
检查更新端口表项
else//分组类型为数据分组
转入算法 1
else//SFT 表中不存在相关条目
if 分组类型=请求分组 then
//查询 FIB 表
转入步骤 6
else//分组类型为数据分组
//查询 PIT 表
转入步骤 5
5.//查询 PIT 表
if PIT 表中存在相关条目 then
if 分组类型=请求分组 then
检查更新端口表项
else//分组类型为数据分组
在 CS 中缓存相关数据分组并且向下一跳转发
else//PIT 表中不存在相关条目 then
if 分组类型=请求分组 then
//查询 FIB 表
转入步骤 6
else//分组类型为数据分组
丢弃数据分组
6.//查询 FIB 表
if FIB 表中有相关信息 then
向下一跳转发
else 丢弃
```

4 仿真与分析

本文实验选择基于 TCP 的区块链^[5]和基于 NDN 批量同步网络内区块的 BlockNDN^[9],在仿真中将本文方法记为“BlockQoS”,实验网络由 7 个区块链节点和 3 个路由器构成,其中包含 2 个边缘节点。各项网络参数设置如表 1 所示。

| 表 1 实验参数设置 | |
|---|-------------------------|
| Table 1 Experimental parameters setting | |
| 参数 | 参数设置 |
| 边缘链路传播时延 | 0~1 ms 内随机值 |
| 核心链路传播时延 | 0~3 ms 内随机值 |
| 逐跳处理时延与排队时延 | 满足均值为 0、方差为 10 ms 的正态分布 |
| 区块产生方式 | 任意节点随机产生 |
| 节点算力顺序 | 随机排序 |
| 区块(交易)轮询周期/ms | 100 |
| 区块生成时间 | 10~15 min 内随机值 |

不同的区块链应用场景对时延敏感程度不同,针对性地设置转发队列入队比例能够更好地满足不同应用场景的 QoS 需求。本文设置网络中时延较敏感数据(包括交易和区块)和时延较不敏感数据(包括交易和区块)的数量比例为 3:1,设置不同的入队比例 $a:b$, a 代表时延较敏感类数据的入队量, b 代表时延较不敏感类数据的入队量,以验证排队策略的性能。设置 $a:b$ 为 1:1 表示不采用排队机制,设置 $a:b$ 为 3:1 验证排队策略对性能的提升作用。在一定时间 $\Delta t(6\times 10^3\text{ s})$ 内,记录在 2 种不同的入队比例下 DDPT 上任意区块链节点产生的所有交易和区块被所有其他区块链节点获取到所花费的时间。实验共进行 100 次,结果取平均值。

图 4 所示为 2 种不同的入队比例下,在特定时间段内网络中所有节点产生的交易或者区块被其他节点同步所耗费的时间。从图 4 可以看出:随着区块数量的增加,不采用排队策略(即对网络中所有交易和区块进行统一转发)所消耗的时间明显高于采用排队策略所消耗的时间;采用和网络中数据类型同样比例进行排队转发的方法,其性能表现出明显的优势,并且随着实验的进行,区块数目越多,优势越明显。

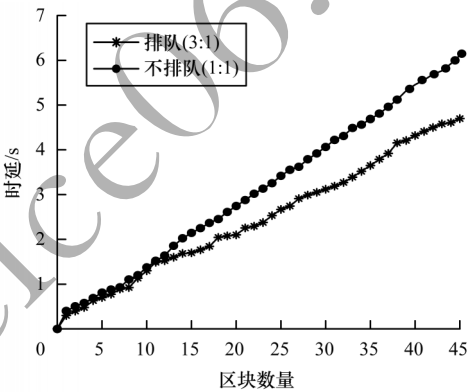


图 4 排队策略对时延的影响

Fig.4 Influence of queuing strategy on delay

设置一个区块的生成时间为 10~15 min 内的随机值,图 5 所示为在形成区块链过程中不同网络中的流量占比。从图 5 可以看出:传统基于 TCP/IP 的区块链网络内存在大量冗余数据包,不同节点对同一个数据内容的请求是独立的,即网络中存在大量对于同一个数据内容的重复请求;BlockNDN 利用了 NDN 网络内缓存的特性,采用批量同步的方式使得网络中的节点可以快速同步交易和区块,但网络中的流量没有被均匀分散到网络各处,导致一些交易或者区块在传输过程中因为网络拥塞而发生丢包或者过期现象,数据的重传带来了额外的流量;本文利用 NDN 支持多播,并且为不同的数据类型创建 DDPT,使流量尽可能地均匀分布,提高了网络资源利用率,相比基于 TCP 的区块链网络,本文方法的网内流量约降低 24%。

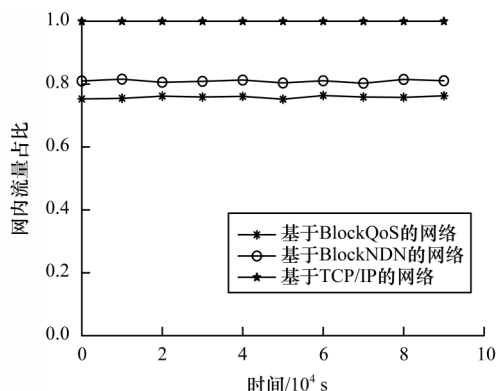


图5 形成区块链过程中不同网络中的流量占比

Fig.5 Proportion of traffic in different networks during the formation of blockchain

图6所示为3种不同网络中所有区块链节点生成的区块全网同步所消耗的时间情况。为验证本文排队策略的性能优势,本次实验仍设定网络中时延较敏感数据(包括交易和区块)和时延较不敏感数据(包括交易和区块)的数量比例为3:1,转发入队比例也为3:1。从图6可以看出:当区块数量较少时,网络资源较为充足,链路拥塞可能性较小,在3种网络中同步区块消耗的时间较为接近,DDPT和比例入队的性能优势没有完全体现出来;随着网络中区块数量的增多,3种网络所消耗的时间出现了较为明显的差异,并且网络中区块数量越多,本文排队策略的优势越明显。

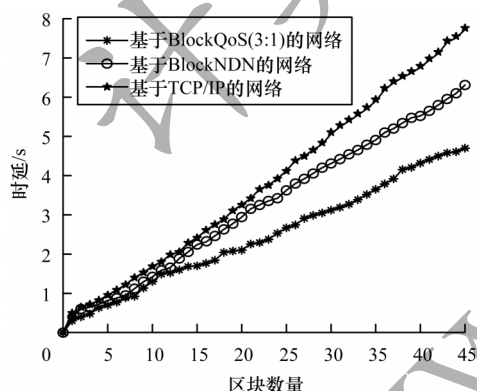


图6 3种网络中全网同步所有区块所消耗的时间情况

Fig.6 Time consumed by the whole network to synchronize all blocks in the three networks

5 结束语

本文提出一种基于NDN的区块链差异化QoS保障方法,利用在TCP/IP体系下较为成熟的差异化服务的思想,结合NDN基于数据名称路由和网络内缓存的优势,为区块链应用场景提供更加有针对性的差异化QoS保障。实验结果验证了该方法的有效性。下一步将从带宽、吞吐量、并发性等方面优化区块链网络层的性能,从而为不同的应用场景提供更加精细和多样的服务。

参考文献

- [1] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494. (in Chinese)
- [2] 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. (in Chinese)
- [3] 刘江, 霍如, 李诚成, 等. 基于命名数据网络的区块链信息传输机制[J]. 通信学报, 2018, 39(1): 24-33.
LIU J, HUO R, LI C C, et al. Information transmission mechanism of blockchain technology based on named-data networking [J]. Journal on Communications, 2018, 39(1): 24-33. (in Chinese)
- [4] TSCHORSCH F, SCHEUERMANN B. Bitcoin and beyond: a technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2084-2123.
- [5] ZHENG Z, XIE S, DAI H, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]// Proceedings of the 6th IEEE International Congress on Big Data. Washington D. C., USA: IEEE Press, 2017: 557-564.
- [6] YUAN H, TIAN S, CROWLEY P. Scalable NDN forwarding: concepts, issues and principles[C]// Proceedings of International Conference on Computer Communications & Networks. Washington D. C., USA: IEEE Press, 2012: 1-9.
- [7] GUO J, WANG M, CHEN B, et al. Enabling blockchain applications over named data networking[C]// Proceedings of 2019 IEEE International Conference on Communications. Washington D. C., USA: IEEE Press, 2019: 1-6.
- [8] SEDKY G, MOUGY A E. BCXP: blockchain-centric network layer for efficient transaction and block exchange over named data networking[C]// Proceedings of 2018 IEEE Conference on Local Computer Networks. Washington D. C., USA: IEEE Press, 2018: 449-452.
- [9] TONG J, XIANG Z, LIU Y, et al. BlockNDN: a Bitcoin blockchain decentralized system over named data networking [C]// Proceedings of the 9th International Conference on Ubiquitous & Future Networks. Washington D. C., USA: IEEE Press, 2017: 75-80.
- [10] HAO W F, ZENG J J, DAI X H, et al. Towards a trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast[J]. IEEE Transactions on Network and Service Management, 2020, 17(2): 904-917.
- [11] JIN H, DAI X, XIAO J. Towards a novel architecture for enabling interoperability amongst multiple blockchains[C]// Proceedings of 2018 IEEE International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2018: 1203-1211.
- [12] ZHONG X, LU R, LI L, et al. DSOR: a traffic-differentiated secure opportunistic routing with game theoretic approach in MANETs[C]// Proceedings of 2019 IEEE Symposium on Computers and Communications. Washington D. C., USA: IEEE Press, 2019: 12-22.
- [13] LI M, ZHU L, ZHANG Z, et al. Anonymous and verifiable reputation system for E-commerce platforms based on blockchain[EB/OL]. [2021-05-20]. http://pure.tudelft.nl/ws/portalfiles/portal/99240287/Anonymous_and_Verifiable_Reputation_System_for_E-commerce_Platforms_based_on_Blockchain.pdf.

(下转第53页)

(上接第 46 页)

- [14] VIRIYASITAVAT W, XU L D, BI Z, et al. Managing QoS of Internet-of-things services using blockchain[J]. IEEE Transactions on Computational Social Systems, 2019, 6(6): 1357-1368.
- [15] CANSEVER A, OZEL U, AKIN O. A distributed message queuing mechanism for a mailing system with high performance and high availability[C]//Proceedings of the 6th International Conference on Control Engineering & Information Technology. Washington D. C. , USA: IEEE Press, 2018; 1-5.
- [16] YANG Z P, HUA L, GAO N J, et al. An accelerating approach for blockchain information transmission based on NDN[J]. Future Internet, 2021, 13(2): 47-48.
- [17] DOKU R, RAWAT D B, GARUBA M, et al. Fusion of named data networking and blockchain for resilient Internet-of-battlefield-things[C]//Proceedings of 2020 IEEE Annual Consumer Communications & Networking Conference. Washington D. C. , USA: IEEE Press, 2020; 1-6.
- [18] LEI K, ZHANG Q, LOU J, et al. Securing ICN-based UAV ad hoc networks with blockchain[J]. IEEE Communications Magazine, 2019, 57(6): 26-32.
- [19] CHEN C, WANG C, QIU T, et al. Secure content sharing scheme based on blockchain in vehicular named data networks[J]. IEEE Transactions on Industrial Informatics, 2020, 16(5): 3278-3289.
- [20] LOU J, ZHANG Q, QI Z, et al. A blockchain-based key management scheme for named data networking [C]// Proceedings of 2018 IEEE International Conference on Hot Information-Centric Networking. Washington D. C. , USA: IEEE Press, 2018; 141-146.
- [21] ZHU K, CHEN Z, YAN W, et al. Security attacks in named data networking of things and a blockchain solution[J]. IEEE Internet of Things Journal, 2019, 6(3): 4733-4741.
- [22] LU W, REN Z, XU J, et al. Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1246-1259.

编辑 吴云芳