

ISSN 2096-742X
CN 10-1649/TP文献DOI:
10.11871/jfdc.issn.
2096-742X.2020.
05.005文献PID:
21.86101.2/jfdc.
2096-742X.2020.
05.005

页码: 41-51

开放科学标识码
(OSID)

基于区块链的软件定义广域网系统研究与设计

庄丽婉¹, 金韬¹, 张晨^{2*}, 黄韬³

1. 东南大学网络空间安全学院, 江苏 南京 210096
2. 网络通信与安全紫金山实验室, 江苏 南京 211111
3. 北京邮电大学, 北京 100876

摘要: 【背景】软件定义广域网 (SD-WAN) 可有效解决传统的企业级广域网成本贵、部署难的问题, 但目前用户在使用SD-WAN时面临着运营商锁定的问题, 在一定程度上制约了SD-WAN的发展。【目的】为SD-WAN提供平台化的接入调度与自动化的结算方案, 解除用户面临的运营商锁定问题。【方法】通过SD-WAN与区块链技术相结合, 本文提出了基于区块链的SD-WAN业务系统, 利用联盟链框架, 针对认证授权、流量调度、结算监管等流程进行了设计, 并通过改进的共识算法增强系统的吞吐量。通过本系统, 用户能够提出个性化的广域网服务需求, 由系统在用户与不同的运营商间进行自动化的、不可篡改的流量调度与结算, 当运营商发生违约时, 用户流量可在运营商间自动切换。【结论】本系统有效解决了SD-WAN运营商锁定的问题, 区块链在网络运营方面体现出了巨大的应用潜力。

关键词: 区块链; SD-WAN; 智能合约; 自动结算

Research and Design of SD-WAN System Based on Blockchain

Zhuang Liwan¹, Jin Tao¹, Zhang Chen^{2*}, Huang Tao³

1. School of Cyber Science and Engineering Southeast University, Nanjing, Jiangsu 210096, China
2. Purple Mountain Laboratories, Nanjing, Jiangsu 211111, China
3. Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: [Background] Software defined wide area network (SD-WAN) can effectively solve the problems of expensive and difficult deployment of traditional enterprise-level WAN. However, the network provider lock-in problem restricts SD-WAN to a certain extent for user development. [Objective] The purpose of the research is to provide a platform-based access scheduling and automated settlement solution for SD-WAN, and to release the lock-in problem faced by users. [Methods] This paper proposes a blockchain-based SD-WAN business system, which uses the alliance chain framework to design authentication, authorization, traffic scheduling, settlement supervision and other processes. Moreover, the throughput of the system can be enhanced through improved consensus algorithms. [Results] On this system, users can customize WAN services that shift between different operators automatically with non-tamperable traffic scheduling and settlement. [Conclusions] This system solves the lock-in problem of SD-WAN effectively, and the blockchain technology shows great application potential in network operation.

Keywords: blockchain; SD-WAN; smart contract; automatic settlement

*通讯作者: 张晨 (E-mail: zhangchen@pmlabs.com.cn)

1 研究背景与相关技术

1.1 软件定义广域网

在广域网场景, 企业与运营商连接一般使用专用的多协议标签交换 (Multi-Protocol Label Switching, MPLS) 电路来帮助确保安全性和可靠性^[1]。但是 MPLS VPN (Virtual Private Network) 专线存在运营商锁定、可控能力不灵活、价格昂贵等缺点。

在云计算、云网一体化的趋势下, 软件定义广域网 (Software Defined Wide Area Network, SD-WAN) 的出现解决了当前对传统广域网的挑战。软件定义网络 (Software Defined Network, SDN) 通过将控制平面和数据平面分离以及开发可编程的优势, 实现网络更好的灵活性、高效性和可控性^[2], 而 SD-WAN 是将 SDN 技术应用于广域网上所形成的一种服务。SD-WAN 通过对网络设备的转发与控制进行分离, 简化了企业级广域网的管理与维护。类似于 SDN 通过虚拟化技术, 增强对于数据中心的管理与维护。SD-WAN 允许企业利用低成本、易获得的 Internet 接入能力, 构建企业级广域网, 降低对于昂贵的传统企业 WAN 连接技术的依赖性。SD-WAN 用户能够通过隧道技术快捷方便地接入 SD-WAN 运营商, 减少了传统 MPLS VPN 专线的昂贵费用。但是由于大多数的 SD-WAN 控制器与 CPE (Customer-Premises Equipment) 设备紧耦合, 以及用户切换运营商时, 双方存在不可信问题, 极有可能出现流量信息的篡改, 因此目前用户在使用 SD-WAN 时面临着运营商锁定的问题, 无法满足敏捷化部署与个性化网络服务, 在一定程度上制约了 SD-WAN 的发展。

1.2 区块链

区块链 (Blockchain) 是一种由多方共同维护, 利用密码学来保证传输和访问安全, 能够实现数据一致存储、难以篡改、防止抵赖的分布式账本技术^[3]。

区块链本质的特征就是在一个分布式系统中无须通过中心节点的控制即可使各节点保持数据的一致性, 因此具有高可靠性、透明可信、不可伪造和防篡改的优势。

1.2.1 区块链部署模式

根据不同应用场景和设计体系, 区块链系统采用不同的开放共享和节点准入方案^[4]。一般来说, 区块链系统有三种部署模式^[5], 包括公有链、联盟链和私有链, 其中联盟链由一组具有共同利益的特定用户群体使用, 对节点具有访问限制, 仅有授权节点可接入, 经过授权的节点可按规则参与共识和数据的读写。联盟链的共识机制^[4]更偏向于效率, 是一种弱中心化的模式, 更适用于企业间的业务需求。

1.2.2 区块链核心技术

(1) 共识机制

共识机制用于解决区块链全网节点数据的一致性问题。区块链作为大规模分布式系统, 为保证所有节点的数据一致需要考虑运行环境的影响。例如公有链是完全暴露在不可信的环境中, 而联盟链或者私有链由于增加了节点准入功能, 环境相对可靠, 但在特定的业务场景中也可能存在不可信问题^[6]。

(2) 智能合约

智能合约是一种能够自动执行条款的数字合约。在区块链系统中, 智能合约实质上是一段计算机代码, 运行在区块链虚拟机或容器中, 可以被预定事件触发后自动执行, 并且执行结果不可被篡改^[7]。用于编写智能合约的语言都是图灵完备的, 因此理论上用户可以实现任何想要实现的业务功能, 使得区块链从主要用于记录电子现金转账的“专有账本”, 升级为可记录计算状态的“通用账本”。

(3) 区块链隐私

区块链的隐私性可以分为两类: 交易数据的隐匿和身份的隐匿^[8]。目前实现区块链隐私计算的主要技术有: 零知识证明、安全多方计算、可信计算环境等^[9]。零知识证明可以保护用户的身份隐私,

安全多方计算可以保护交易数据的隐私, 而安全芯片可以保证合约代码的隐秘性。其中用到的密码学技术包括同态加密、可搜索加密、特殊性质签名等。

1.3 区块链在软件定义广域网的应用场景分析

在区块链技术与 SD-WAN 技术方面, 两者的融合将加速双方发展。传统网络存在静态部署、部署周期长、费用昂贵等问题, 这对区块链网络的部署与通信存在制约。区块链网络需要部署可靠、低成本、对所有用户可用的公共互联网链路。由于 SD-WAN 支持实时应用程序性能与可预测的服务保障区块链的网络部署可通过 SD-WAN 技术进行优化。而在 SD-WAN 研究中, 研究人员也积极地将区块链技术应用到 SD-WAN 中。由于 SD-WAN 网络易受到攻击, 可在 SD-WAN 应用层与控制层之间增加区块链层^[10]。通过区块链的不可篡改性、分布式存储、多方共识机制保证 SD-WAN 网络数据的安全性、可靠性。

在通信领域, 电信运营商正在积极利用自身在网络资源和终端资源上的优势, 布局区块链新型生产模式^[11], 国内外主流电信运营商均已布局区块链相关业务, 尤其在移动通信的漫游场景已经得到广泛的研究^[12]。例如, 在传统漫游通信中, 网络运营商面临着漫游合同数量多, 部署困难, 结算无法自动化等问题^[13]。尤其当物联网漫游和 5G 应用更加普遍时, 这些问题将更加突出。2020 年 2 月, Telekom 创新实验室基于联盟链构建电信漫游业务系统, 简化网络运营商之间在批发漫游、批发语音和按需数据领域中的商业用例流程, 在运营商间可多方互信地实现自动化业务流程, 为移动用户提供更好的通信服务。

参考移动通信的漫游场景, SD-WAN 用户通过隧道接入 SD-WAN 运营商, 技术上也可以通过灵活

的调度来在运营商之间进行切换, 但目前将用户在不同运营商间进行调度时存在流量调度与统计信息不互信的情况, 极有可能发生流量信息的篡改, 因此用户在使用 SD-WAN 时只能选定在一家运营商, 导致了较为明显的运营商锁定问题。为解决不互信的问题, 本文探索了基于区块链的软件定义广域网业务系统, 可有效解决用户与多个运营商之间认证、合同签订、部署以及资费结算等问题, 并可通过改进的共识算法增强系统的吞吐量。

2 系统架构设计

本文提出了一种基于区块链的软件定义广域网业务系统, 使用联盟链的部署模式, 提供准入功能, 通过智能合约自动结算金额, 降低成本提高效率。从业务主体上看, 本系统共有用户、运营商和第三方机构三大主体。从系统模块组件上看, 可以分为非区块链部分与区块链部分, 模块组成如下图 1 所示。

2.1 区块链部分

本系统采用联盟链的部署模式, 区块链的参与主体有运营商、用户与第三方。区块链主要负责合同签订、调度与网络质量信息记录、自动化结算。

2.1.1 区块链部署模式

智能合约是运行在区块链虚拟机或容器中的一段代码, 用于控制交易过程, 保证交易数据的一致性、完整性。在本系统中, 用于实现用户与运营商之间的签约与结算、身份校验授权、数据调差、作恶罚处等业务功能。智能合约按功能划分, 具体如下:

(1) 身份校验、授权鉴权模块: 负责鉴定用户与运营商读写权限。

(2) 签约模块: 负责多方合同的签订。

(3) 记账模块: 负责调度过程中, 从采集系统中获取调度与网络质量记录等。

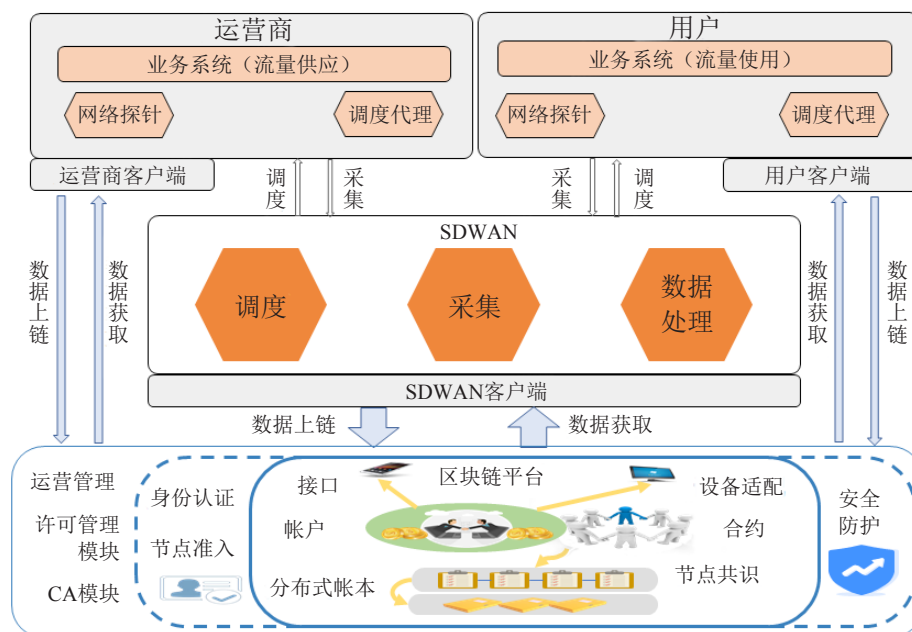


图1 系统架构图

Fig.1 System architecture diagram

(4) 结算模块：负责结算用户与运营商之间的账单。

(5) 罚处模块：负责记录运营商、第三方和用户的违规情况，用作后期惩罚的凭证。

2.1.2 区块链调度模式

在调度过程中，SD-WAN 调度器中调度模块向区块链获取签约数据，采集模块与数据处理模块向区块链推送调度与网络质量信息。区块链根据选取的共识算法，通过一方记账两方验证的方式，保证上链信息的正确性。区块链的链式结构保证上链信息的不可篡改性、可追溯性，为自动化结算提供了数据来源。

2.1.3 自动化结算

用户和运营商客户端将流量与价格数据上传区块链，同时 SD-WAN 客户端将网络调度记录上传区块链，所有上链的数据可以作为结算的参数来源，调用智能合约即可完成自动化结算。通过这种方式保证数据的可溯源、不可篡改性以及结算金额的准

确性，同时也便于监管。

2.2 非区块链部分

非区块链部分包括运营商与用户的业务系统、客户端、SD-WAN 组件和运营管理模块四大部分。其中，运营商与用户分别是网络流量的提供方和使用方，SD-WAN 核心组件以及运营管理模块可以交由第三方机构管理。

SD-WAN 负责根据签约数据以及网络质量情况进行智能化地网络调度。组件可分为调度、采集、数据处理、网络探针和调度代理五个部分，其中调度模块负责网络调度，采集模块负责两端的实时流量采集，数据处理模块负责调度与采集间的数据处理。另外，网络探针与调度代理部署在用户以及运营商设备上。

运营管理模块是一个中心化的系统，为区块链提供运营维护功能，负责成员身份认证、许可准入管理，节点、应用准入管理，通过 CA（Certificate Authority）子模块对认证成功的账户或节点签发签

名证书、通信证书、服务证书, 并负责证书的管理。

客户端是与区块链交互的媒介, 用户通过客户端注册区块链账户, 通过录入身份信息或单位资质信息等进行身份认证, 认证通过后获得用户准入证书, 方可调用区块链轻节点连入区块链网络。

3 系统功能模块与流程

本系统联盟链功能模块可分为许可管理、签约调度、资费结算、数据调整四个环节, 具体展开如下。

3.1 许可管理

认证与授权是联盟链平台不可或缺的功能, 基于区块链的软件定义广域网业务系统旨在搭建联盟链平台, 控制用户、应用、节点的准入, 对想要加入平台的区块链用户及其部署的节点进行身份认证与权限管理, 打造可信的交易环境。用户与节点需

要通过准入证书, 在区块链中进行签名认证; 用户登陆区块链的设备应用, 如客户端与节点设备需要加载通信许可、服务许可等 CA 证书才能在区块链中进行通信, 提供服务。

在系统中, 认证即加入到区块链的所有用户以及他们所拥有的节点进行身份信息审核, 包括身份证号、机构代码、相关资质等, 审核通过后调用 CA 系统为用户或节点颁发证书, 赋予其进入区块链网络的权限。如下图 2 所示, 为本系统的许可管理功能模块设计图。

3.2 签约调度

首先运营商进行区块链许可管理流程, 通过接入端连接到区块链平台, 当运营商加入平台时, 运营商与第三方机构签署网络质量合同, 合同记录了网络质量参数以及价格结算方式, 签署完成后运营商即加入本平台, 合同上传至区块链平台。然后用

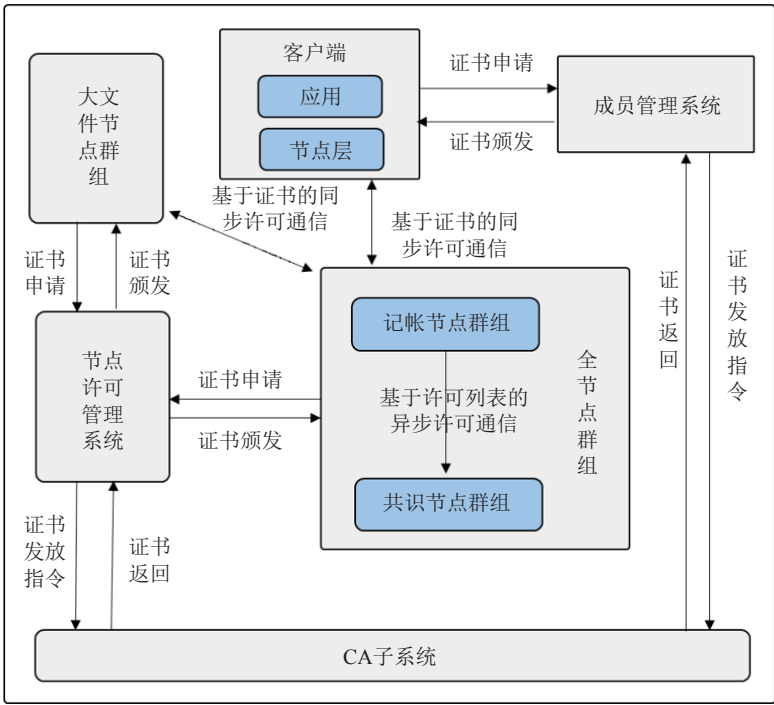


图 2 许可管理功能模块

Fig.2 License management function module

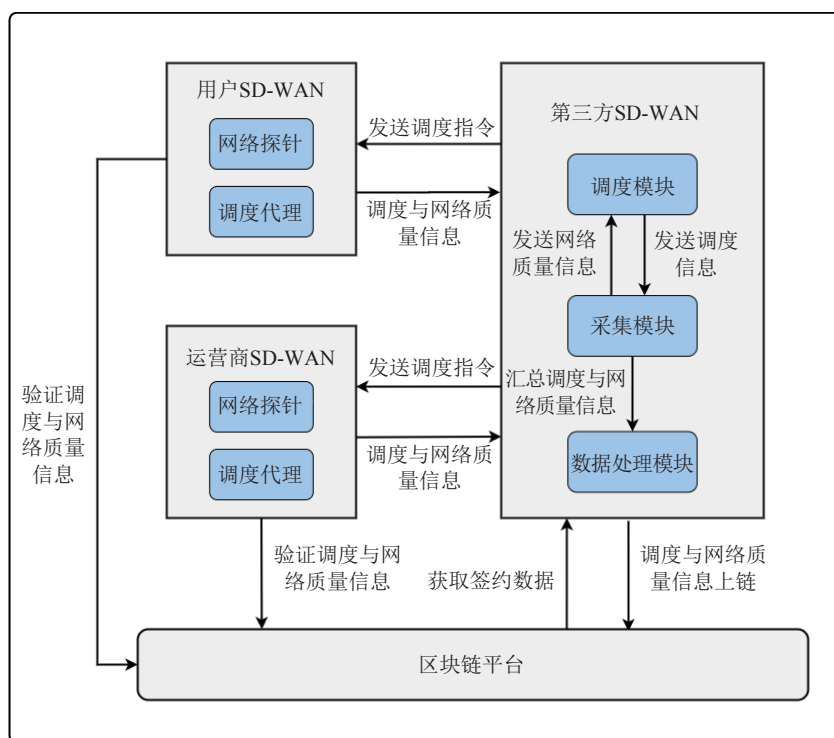


图 3 SD-WAN 采集与调度

Fig.3 SD-WAN collection and scheduling

户进行区块链许可管理流程，通过接入端连接到区块链平台，当用户加入平台时，用户与第三方机构签订需求合同，合同记录了用户要求的网络质量参数，签署完成后用户即加入本平台，合同上传至区块链平台，同时生成的智能合约还提供了结算、调差、惩处等功能。

签约完成后,SD-WAN 负责根据签约数据以及网络质量情况进行智能化地网络调度。SD-WAN 共包含调度模块、采集模块、数据处理模块。采集模块定时从用户与运营商网络探针获取网络质量数据,并发送给调度模块。SD-WAN 调度器向区块链平台获取签约数据,调度模块依据签约数据与网络质量数据为用户调度最佳运营商。且在通信过程中,调度模块依据从区块链上获取的用户需求合约数据与采集模块实时推送的网络调度质量数据,判断用户目前的所连接的网络运营商提供的网络质量是否符合要求,如果不符合要求,直接从该用户签约的运

营商中筛选最优运营商，进行网络切换。

3.3 资费结算

资费结算过程由运营商发起，运营商使用客户端发起调用智能合约交易，智能合约执行结算模块，能够从账本中读取到这段时间内使用本运营商服务的每个用户所用的流量总额，并分别计算金额，最后将执行结果写入账本中，写入的数据无法被篡改。用户可以根据账本中的金额数据进行外部支付。自此完成这段时间内的自动化资费结算。

选择让运营商去发起结算交易是考虑到本系统的核心目标是让运营商和用户做点对点结算，而第三方机构在其中只是担任监管和提供服务的角色。因此主动权还是在用户与运营商，但是由于用户的设备层次不齐，所以运营商承担了主要的结算主动权。资费结算具体如图4。

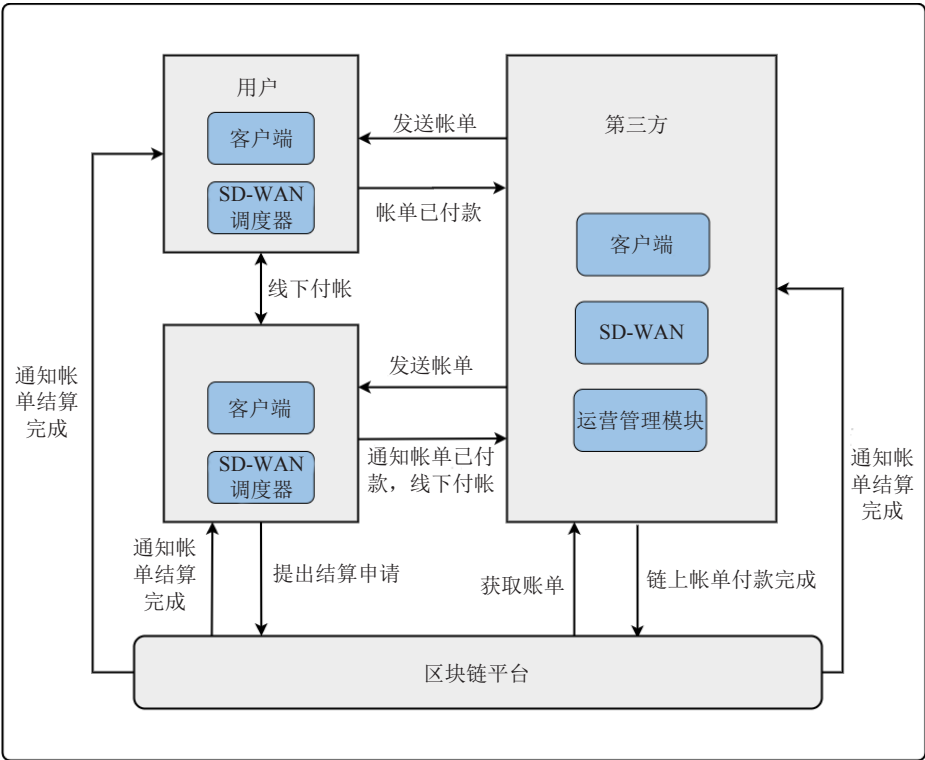


图 4 资费结算

Fig.4 Tariff settlement

3.4 数据调整

在系统运行的过程中，有些数据需要调整，如用户需求参数的更改、运营商网络服务参数与价格的更改、错误数据上链的更正以及对运营商的惩处。

3.4.1 调整需求参数

用户的需求合同中会有一个时间期限，这个期限是由双方进行协商的，在这个期限内用户无法改变自己的需求参数，这是为了保证运营商的利益以及系统的效率。当过了这个期限，用户可以申请调整需求参数。

3.4.2 调整网络服务参数

运营商的网络质量合约中也有一个时间期限，这个期限是由双方进行协商的，但考虑到运营商网络的特殊性，若有突发状况导致需要临时修改参数，可以向第三方申请，审核通过后方可进行调整。另外，

在突发情况下，运营商可提出申请紧急更改网络服务参数。但运营商紧急申请有一定次数限制，且外部审核通过后才可更改。用这种方式可以使运营商在突发情况时可以不考虑当前合约的时间期限，直接向第三方申请调整网络质量参数。

3.4.3 更改错误数据

用户或运营商在发现流量或结算数据问题后，向第三方报告，第三方分别向调度模块与采集模块发送核实情况请求，调度模块与采集模块通过本地缓存记录核实相关情况，再将核实结果发送给监管部门，第三方根据调查情况调用智能合约，智能合约执行调差模块，调差数据写入账本，第三方通知用户或运营商对此事件的处理结果。

3.4.4 惩处过程

用户发现运营商提供的网络不稳定或存在质量

问题后, 向第三方报告。第三方可以通过三种方式来核实情况, 分别为: (1) 向运营商探针核实网络质量情况; (2) 向采集模块核实当时网络质量情况; (3) 同时向运营商传感器与采集模块核实情况。第三方选取一种方式进行核实, 待收到网络质量情况后, 进行分析判断, 再调用智能合约, 智能合约执行惩处模块, 生成惩处合约交易, 惩处记录写入账本后, 第三方会通知用户和运营商处理结果。而且, 在一段时间内, 调度模块会减少有问题的运营商提供服务的几率, 作为提供不符合网络质量要求的惩处。

4 系统共识算法优化

4.1 共识算法比较与分析

分布式系统的共识达成需要依赖可靠的共识算法, 共识算法通常解决的是分布式系统中由哪个节点发起提案, 以及其他节点如何就这个提案达成一致的问题。联盟链主流的共识算法有 PBFT (Practical Byzantine Fault Tolerance)、Raft、DPoS (Delegated Proof of Stake) 等, 具体机制与优缺点如下表 1 所示。

表 1 联盟链共识机制

Table 1 Alliance Chain Consensus Mechanism

共识机制	核心思想	优点	缺点
PBFT	主节点排序请求, 从节点响应请求, 多数节点响应结果为最终结果	可解决拜占庭故障问题, 共识结果的一致性与正确性程度高, 共识达成时间快	去中心化程度不足, 多中心化机制, 算法复杂度高, 当节点数量过多时, 运行效率较低
Raft	通过分布式节点选举出的领导人节点得到区块记账权	共识结果的一致性和正确性程度高, 可达到秒级验证	去中心化程度不足, 多中心化机制, 算法复杂度较高
DPoS	通过股东投票方式选出代表得到记账权	大幅度缩短共识达成时间, 可达到秒级验证	无法完全去中心化, 若节点数量过少, 投票选出的代表节点代表性不强

4.2 共识算法的选取与优化

在本系统中是基于联盟链的设计, 但是由于网络调度这一特殊的应用场景, 且希望有更多的用户与运营商加入到这一系统中, 因此在设计时, 无法彻底排除作恶节点的存在。所以, 本系统采用了能够容纳故障节点, 也能容纳作恶节点的 PBFT 共识算法。

PBFT 算法能容纳故障节点与作恶节点, 安全性高, 采用加密技术防止欺骗攻击与重放攻击。算法共识效率高, 共识时延约在 2-5 秒, 可基本达到商用实时处理要求, 满足高频交易量需求。但 PBFT 算法无法高效地使大量节点达成共识, 当共识节点数量较多时, 运行效率较低。

为解决 PBFT 共识算法在节点数量较多的情况下, 效率会大大降低这一缺点, 我们对共识算法进行了优化。根据 DPoS 的思想, 提出了适用于本系统的 DPoA (Delegated Proof of Ability) 共识机制。与传统的 DPoS 不同, DPoA 并不是根据矿工持有的代币数量或币龄作为选举标准投票权重, 而是按全节点的存储容量、网络稳定性等指标作为衡量标准, 随机选取共识节点, 获得更好的公平性和网络效率。

本系统采用了 DPoA+PBFT 作为共识算法。PBFT 算法将指数级别的拜占庭协议运行复杂度降低到多项式级别, 实现了在分布式环境下, 节点强一致性和高效率的共识。PBFT 算法每秒处理交易的个数 (Transactions Per Second, TPS) 约为 400-800, 与比特币 7TPS、以太坊区块链约 20TPS 相比, 效率大大提高。而 DPoA 算法解决了 PBFT 算法共识节点多、效率大大降低的问题, 得到更高的可用性, 也进一步提升了共识效率。

在业务流程中, 当节点较多时, 采用 DPoA+PBFT 算法, 通过 DPoA 算法选取共识节点, 之后再通过 PBFT 算法达成共识, 广播新区块。而当需要达成共识的节点较少时, 只需采用 PBFT 达成共识。下图 5 为 DPoA+PBFT 共识算法示意图。

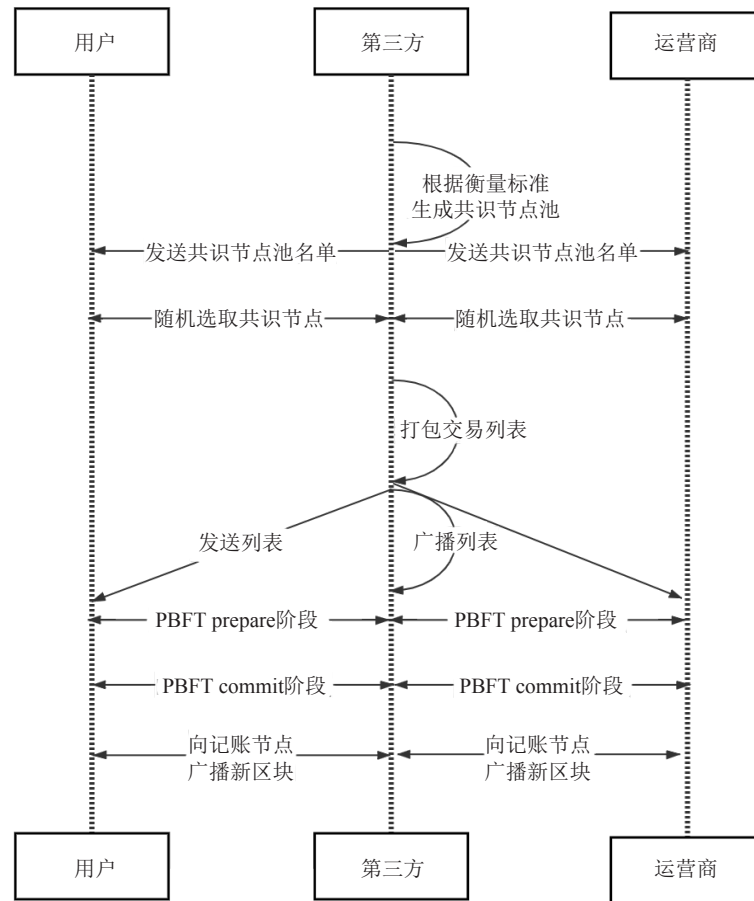


图 5 DPoA+PBFT 共识

Fig.5 DPoA + PBFT hybrid consensus

5 总结与展望

本文提出了一种基于区块链的软件定义广域网业务系统, 并通过 SD-WAN 与区块链技术相结合给出了具体的系统架构。思路, 利用区块链对于数据存证的不可篡改的特性, 对于多方间的调度和采集数据进行可信存证, 解决了将用户流量在多个运营商间调度时的互不信任问题。这需要对于传统网络以及 SD-WAN 的签约、调度、采集和结算等业务功能模块与接口流程等方面进行重构。为了在实现相关功能的同时兼容传统网络与 SD-WAN, 本系统将区块链平台与 SD-WAN 进行了松耦合的设计, 保留了 SD-WAN 与用户 / 运营商设备间的控制接口, 以及用户设备与运营商设备间的数据接口, SD-

WAN 以及用户 / 运营商设备作为客户端与区块链通信进行数据的上链与获取。不过, 虽然松耦合的方式下兼容性较高, 但 SD-WAN 的调度算法并未实现上链, 未来将考虑通过智能合约的方式可信地运行 SD-WAN 的调度算法, 但由于 SD-WAN 的调度算法非常复杂, 在智能合约上运行会导致调度算法性能的大幅降低, 未来的工作方向上, 可基于此问题进行深入研究。

另外, 在系统的安全隐私等方面, 后续可将零知识证明、同态加密等技术与系统融合, 实现数据加密与身份隐匿, 提高系统的隐私性; 以及许可管理多级 CA 的具体架构、黑名单与白名单的详细设计等问题。

利益冲突声明

所有作者声明不存在利益冲突关系。

参考文献

- [1] E. K. Ali, M. Manel and Y. Habib, An Efficient MPLS-Based Source Routing Scheme in Software -Defined Wide Area Networks (SD-WAN)[C]. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, 2017, pp. 1205-1211.
- [2] Z. Yang, Y. Cui, B. Li, Y. Liu and Y. Xu, Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities[C]. 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 2019, pp. 1-9.
- [3] 中国信息通信研究院.可信区块链推进计划. 区块链白皮书(2019)[EB/OL]. <http://www.caict.ac.cn/kxyj/qwfb/bps/201911/P020191108365460712077.pdf>.
- [4] 何宝宏,魏凯,和涛.公有链白皮书(2019) [EB/OL]. <https://img.jinse.com/1879734.pdf>.
- [5] 中国区块链技术和产业发展论坛标准. 区块链参考架构[S].CBD-Forum-001-2017.[6] 刘懿中,刘建伟,张宗洋,徐同阁,喻辉. 区块链共识机制研究综述[J].密码学报,2019,6(04):395-432.
- [7] Sillaber, C., Walth, B. Life Cycle of Smart Contracts in Blockchain Ecosystems. Datenschutz Datensich 41, 497-500 (2017).<https://doi.org/10.1007/s11623-017-0819-7>.
- [8] 张宪,蒋钰钊,闫莺. 区块链隐私技术综述[J].信息安全研究,2017,3(11):981-989.
- [9] 周李京. 区块链隐私关键技术研究[D].北京邮电大学,2019.
- [10] 陈龙. 基于区块链的轻量级SDN应用层研究[D].浙江工商大学,2019.
- [11] 张小军,曹朝,胡瑞丰. 华为区块链白皮书(2018) [EB/

OL]. https://developer-res-cbc-cn.obs.cn-north-1.myhuaweicloud.com/upload/files/pdf/20180411/2018041144924_27164.pdf.

- [12] 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(04):481-494.
- [13] 孙洁. 电信结算现状及前景分析[J].通信与信息技术,2018(04):70-71+55.

收稿日期: 2020年4月22日

庄丽婉, 东南大学网络空间安全学院研究生。主要研究方向为区块链、未来网络体系架构、软件定义网络等。本文主要承担工作为系统的功能模块与流程设计、共识算法选取与优化, 以及论文撰写。



Zhuang Liwan is currently a graduate student of the School of Cyber Science and Engineering Southeast University. Her main research directions are blockchain, future network architecture and software-defined network, etc.

In this article, she is mainly responsible for the system's functional modules and process design, consensus algorithm selection and optimization, and thesis writing.

E-mail: zhuangliwan@seu.edu.cn

金韬, 东南大学网络空间安全学院研究生。主要研究方向为区块链、未来网络体系架构、软件定义网络等。本文主要承担工作为文献调研、系统架构设计, 以及论文撰写。



Jin Tao is currently a graduate student of the School of Cyber Science and Engineering Southeast University. His main research directions are blockchain, future network architecture and software-defined network, etc.

In this article, he is mainly responsible for literature research, system architecture design, and thesis writing.

E-mail: cat_jintao@seu.edu.cn

张晨, 南京网络通信与安全紫金山实验室, 主要研究方向为未来网络体系架构、软件定义网络、云网融合、云原生网络等。

本文主要承担工作为对系统整体设计提出指导意见, 对文章框架、内容进行修改。

Zhang Chen graduated from Beijing University of Posts and Telecommunications. He is a future network researcher at the Purple Mountain Laboratory in Nanjing Network Communication and Security. His main research directions are future network architecture, software-defined network, cloud-network integration and cloud-native network, etc.

In this article, he is mainly responsible for the overall system



design guidance, and article revision.

E-mail: zhangchen@pmlabs.com.cn

黄韬, 北京邮电大学, 教授, 博士生导师, 主要研究方向为未来网络体系架构、软件定义网络、确定性网络、大规模网络试验平台等。

本文中为文章整体框架进行总体指导。

Huang Tao is a professor and doctoral supervisor at Beijing University of Posts and Telecommunications. His main research directions are future network architecture, software-defined network, deterministic network, and large-scale network test platform, etc.

In this article, he is mainly responsible for the overall article framework guidance.

E-mail: htao@bupt.edu.cn



引文格式: 庄丽婉, 金韬, 张晨, 黄韬. 基于区块链的软件定义广域网系统研究与设计[J].数据与计算发展前沿,2020,2(5): 41-51.DOI:10.11871/jfdc.issn.2096-742X.2020.05.005.PID:21.86101.2/jfdc.2096-742X.2020.05.005.

Zhuang Liwan, Jin Tao, Zhang Chen, Huang Tao. Research and Design of SD-WAN System Based on Blockchain [J].Frontiers of Data & Computing, 2020,2(5): 41-51.DOI:10.11871/jfdc.issn.2096-742X.2020.05.005.PID:21.86101.2/jfdc.2096-742X.2020.05.005.