计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210500159

区块链即服务平台关键技术及发展综述

毛瀚宇[1]　聂铁铮[1]　申德荣[1]　于　戈[1]　徐石成[2]　何光宇[2]
1 东北大学计算机科学与工程学院　沈阳 110169
2 东软集团股份有限公司技术与战略发展事业部　沈阳 110179
(2010676@stu.neu.edu.cn)

摘　要　区块链即服务是将区块链框架嵌入到云计算平台的一种新型应用方式,能够有效利用云平台提高区块链系统部署和运营的便捷性和高效性。文中主要对区块链即服务(BaaS)的关键技术和现有平台系统进行了全面的分析总结。首先介绍了BaaS的概念和平台功能,分析了BaaS平台在提高安全性能、实现个性定制和降低开发成本等方面具有的优势;然后基于现有商业化BaaS平台详细介绍了BaaS平台的系统架构和关键技术架构,并介绍了当前主流的BaaS平台的特性技术和功能,以及相关应用场景;最后,在整理当前BaaS平台遇到的挑战问题的同时对BaaS的未来研究方向进行了展望。

关键词:区块链;云计算;区块链即服务;跨链;联盟链
中图法分类号　TP315

Survey on Key Techniques and Development of Blockchain as a Service Platform

MAO Han-yu[1],NIE Tie-zheng[1],SHEN De-rong[1],YU Ge[1],XU Shi-cheng[2] and HE Guang-yu[2]
1 School of Computer Science and Engineering,Northeastern University,Shenyang 110169,China
2 Neusoft Corporation Technology and Strategic Development Division,Shenyang 110179,China

Abstract　Blockchain as a Service is a new application method that embeds the blockchain framework into the cloud computing-platform,which can effectively use the cloud platform to improve the convenience and efficiency of the deployment and operation of the blockchain system. This paper mainly analyzes and summarizes the key techniques and existing platform systems of Blockchain as a Service. Firstly,this paper introduces the concept and function of BaaS platform,and analyzes the advantages of BaaS platform in improving safety performance,realizing personalized customization and reducing development cost. Then,based on the existing commercial BaaS platform,the system architecture and key technique architecture of BaaS platform are introduced in detail,and the characteristics,technologies and functions of the current mainstream BaaS platform,as well as the relevant application scenarios are introduced. In this paper,the challenges encountered by the current BaaS platform are summarized,and the future research direction of BaaS is prospected.

Keywords　Blockchain,Cloud computing,Blockchain as a Service,Cross-chain,Consortium blockchain

1　引言

自2008年学者中本聪提出比特币白皮书《Bitcoin:A Peer-to-Peer Electronic Cash System》[1]以来,区块链技术受到大量计算机领域学者所关注,其底层技术包括分布式账本[2]、共识机制[3-4]、智能合约和密码学[5]算法,具有去中心化、不可篡改性、透明性、可溯源性、最终一致性等特点[6-7]。2014年以太坊平台出现,其以智能合约技术(smart contract)拓展了区块链技术的可用性,出现了大量链上应用。同时期Linux基金会的Hyperledger Fabric[8]等项目则构建了区块链应用技术的完整生态环境。当前正处于区块链3.0时代,其范围逐渐深入至金融、医疗、司法、教育、政府、文化、科学等多类型产业,在区块链基础上不同产业融合发展,产生了大量基于区块链技术的去中心化应用[9]。

区块链大型应用项目不断发展,但相关计算机开发人员往往缺少高质量硬件、实用开发工具和相关配套开发环境,因此造成了小型开发团队难以开发、生态内软件断层的情况。因此Microsoft与IBM提出了区块链即服务BaaS(Blockchain as a Service)概念,为开发者提供了一种结合区块链技术的云服务平台。

到稿日期:2021-05-22　返修日期:2021-07-27
基金项目:国家自然科学基金(62072086);辽宁省重点研发计划项目(2020JH2,1010037);中央高校基本科研业务费项目(N2116008);东软集团股份有限公司开放课题(NCBETOP2002)
This work was supported by the National Nature Science Foundation of China(62072086),Key R & D Program of Liaoning Province(2020JH2,1010037),Fundamental Research Funds for the Central Universities (N2116008) and NEUSOFT Open Project(NCBETOP2002).
通信作者:于戈(yuge@mail.neu.edu.cn)

区块链即服务(Blockchain as a Service，BaaS)，结合云计算[10]和区块链技术，将区块链框架、开发工具等嵌入至云计算平台，使用云服务基础设施。用户通过租赁等方式实现高效便捷的区块链生态开发服务，同时支持链上业务运营及业务拓展的区块链云平台技术。BaaS[11]降低了开发者的开发和维护成本，其环境安全可靠，可实现项目的快速部署，给用户提供了链上查询、数据分析、请求交易、跨链访问[12-13]、构建智能合约等多种功能。

开发者基于 BaaS 能够快速构建开发环境，通过云平台提供的接口来实现快速高效的部署，并建立行业的统一标准与规范。BaaS 结合云平台服务技术，给用户提供基于公有链实质性服务，如链上查询、数据分析、构建智能合约[14]，无需开发者构建自己的区块链，在降低开发者开发负担的同时提高了开发应用的安全系数。基于现有的 BaaS 平台的应用情况可以看出，其在应用中具有以下优势：

(1)可靠的安全性

开发者基于 BaaS 的应用框架，如 IBM、蚂蚁金服等企业的 BaaS 平台，利用供应方提供的共识机制[15]、加密算法、隐私保护[16]等开发链上应用，具有较高的技术透明性，能够提高自身开发项目的安全性，同时在宣传推广时期，可提高用户对系统的信任程度。

(2)灵活的个性化定制

BaaS 平台提供了大量模块化的开发工具和接口的标准服务，支持开发者在线配置和自定义的功能扩展，提高了设计灵活性。智能合约引擎的存在适应了实际业务需求复杂多变这一特点，可支持智能合约的可视化编辑、部署与管理，如蚂蚁金服推出的蚂蚁区块链 BaaS 平台支持开发者使用 Solidity[17]和 C++编程语言开发智能合约，同时提供 Java，C++和 JS 的 SDK 接口，实现了合约调用、查询状态、数据查询等功能。

(3)低廉的开发成本

开发成本是衡量项目开发的重要指标之一，BaaS 平台为开发者提供了大量基础设施与实用工具，仅购买服务即可节省大量基础开发成本与时间，同时提高了部署效率和测试速度。BaaS 提供的生态服务环境有利于中小企业及创业者进行相关开发。

本文将对 BaaS 的核心关键技术、现有的主要系统架构进行介绍，并对 BaaS 未来的发展前景和挑战进行了分析。本文第 2 节介绍了 BaaS 核心技术，提出了当前 BaaS 平台的技术优势；第 3 节分析并总结了多个当前的主流 BaaS 平台，展示了 BaaS 平台通用系统架构和技术架构；第 4 节分析了当前的应用现状，介绍了部分当前主流的 BaaS 平台，包括 Oracle Blockchain Platform，Azure，TBaaS 和 Antchain BaaS，并提出了 BaaS 平台适应性良好的部分应用场景，如跨境转账、商品溯源、电子病历、慈善捐款和司法可信存证；第 5 节介绍了 BaaS 平台发展上当前面临的挑战与问题，并提出了 BaaS 平台未来可能的研究方向；最后总结全文并展望未来。

2 BaaS 核心技术

BaaS 平台主要基于云计算框架进行构建，同时利用云服务平台的生态环境集提供服务，其中涉及的关键技术主要包括以下几个方面。

2.1 云计算

在 BaaS 平台中，云计算[18]技术作为最底层服务核心，云计算最大的特点是资源池化，即 BaaS 平台用户不需要考虑设备、内部使用技术以及使用位置，按需购买云计算服务即可。

BaaS 平台使用云服务较为重要的一点就是使用云存储[19]功能。云存储即使用网络在线存储，购买租赁数据存储空间后将数据通过网络存放至第三方托管服务器中，部分 BaaS 平台支持明文数据上传与上链和密文数据上链，保留了传统云服务存储的模式，同时结合了区块链数据[20]上链的特性，保证数据不可篡改和可溯源，又提供了数据加密后上链即密文数据上链，保护了用户的数据隐私安全。部分 BaaS 平台基于联盟链特性还实现了分级密钥，即通过数据导出函数(合约)进行密钥管理，可根据不同权限和分享范围分享密钥与关联数据。

传统云计算需要保证服务的可持续性、安全性、高效性和灵活性，BaaS 平台结合区块链技术的数据不可篡改性、安全性、数据持久性等，进一步降低了云计算服务的成本费用和租赁费用，供应商也不必按照传统模式提供大量设备用于数据备份、冗余管理和安全防护。

2.2 跨链技术

当前大量 BaaS 平台实现了较为成熟的区块链跨链访问技术，除公有链间提供跨链资产传输，联盟链平台已实现跨链信息交互功能，平台内部实现多链架构，部分平台间可以跨平台访问。跨链技术可分为第三方协作交互、区块监听和不直接交互 3 种方式，跨链技术架构模式如图 1 所示。

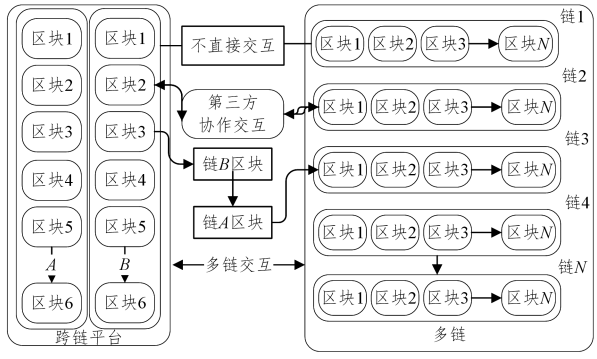

图 1 跨链架构模式图

Fig. 1 Cross-chain architecture

跨链技术可理解为链到链间的通信协议，BaaS 平台常用的跨链技术包括 4 种方法：公证人认证、侧链/中继、分布式私钥控制和哈希锁定。公证人认证[21]即假设发送链 A 和目标链 B 是不能互相信任的，需要一个第三方公证人作为中介介入双方交易，如果对安全性有更高要求，则需要更多第三方公证人。侧链/中继方法[22]是在链上存储其他区块链的区块头物理实现跨链访问。分布式私钥控制技术[23]使用大量分布式节点，使用私钥控制相关资产，且主链资产可被映射至其他各链，部分 BaaS 平台使用改进的分布式私钥控制技术实现了信息和资产的单双向发送。哈希锁定技术[24]使用时间锁和哈希算法实现小规模的跨链资产兑换，如闪电网络技术在

BaaS平台系统繁忙的状态下，提供了快速、安全、可信的链下传输交易通道技术。

跨链技术结合BaaS平台的监管模式，可保证用户跨链访问的信息及资产安全，提高了共识效率，从而进一步提高了跨链技术的效率。通过良好的跨链技术能够大幅提高公有链性能，并提高联盟链上的拓展性。BaaS平台用户仅根据平台提供的接口或智能合约即可实现对其他链的访问，实现平台生态内部的标准性和一致性。

2.3 智能合约

BaaS平台智能合约[25]引擎通常使用智能合约虚拟机及智能合约容器来实现，支持Solodity，Java，JS，C++等多种编程语言。大量基本智能合约代码由平台开发并内置于系统合约容器内，通过接口即可实现调用，BaaS平台通过合约调度机制可实现用户间合约代码共用，以减小系统负担，同时BaaS平台支持用户自定义智能合约，经安全检查认证后自定义智能合约即可上线。大量开放的智能合约实现了BaaS平台的工具性和有效性，也实现了用户个人定制化的需求，部分平台还实现了智能合约的隐私保护。图2给出了智能合约在BaaS平台上的工作原理，其中隐私保护节点由CPU硬件[26]提供保护，具有高度安全隔离和可证明特性。

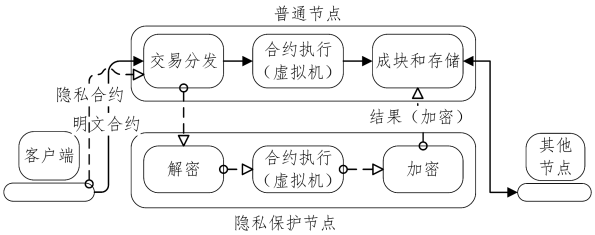

图2 智能合约的工作原理

Fig. 2 Principle of smart contract

2.4 身份认证技术

BaaS平台使用身份容器和身份管理引擎对平台内的用户进行管理，用户可根据平台内的要求申请使用平台相关功能，基于联盟链的BaaS平台为联盟链用户提供了管理功能，包括邀请、冻结、角色配置、成员管理等，任何参与联盟链的机构或个人均需要通过认证流程并由BaaS平台颁发证书，以认证客户在联盟链上的身份，用户可进一步获取相关开发组件，BaaS平台为用户提供整个区块链浏览器和运行状态监控，上述功能为各行业内部实现区块链应用提供了帮助。此外，BaaS平台提供账户映射服务，账户映射服务是一套用于业务账户与链上账户进行映射和托管的服务，通过此服务能够管理业务账户与链上地址的映射关系，能够更安全高效地管理链上账户的公私钥，为等待上链的交易提供签名。

3 BaaS系统架构

本节将从BaaS的平台逻辑架构和技术架构两方面展开，就BaaS平台层次进行分析。

3.1 BaaS平台架构

BaaS系统主要包含应用层、管理层、区块链层和云平台层。图3给出了BaaS平台的系统架构。

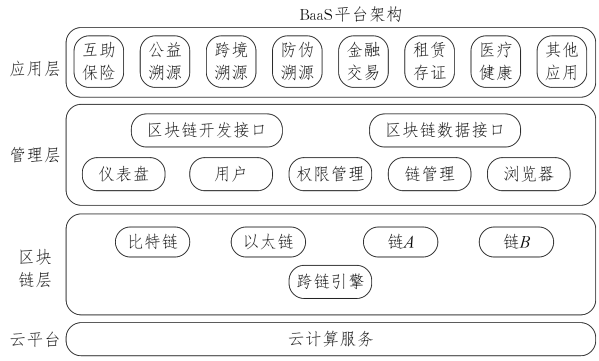

图3 BaaS平台的系统架构图

Fig. 3 BaaS system architecture

应用层包括医疗应用、金融应用、政府政务系统、电商应用等，大量应用由BaaS平台合作方和平台内部用户开发，是基于BaaS平台内部规范和接口开发的，实现了平台内的标准与统一。

管理层将底层功能与服务封装，开放为标准化接口，其中包括区块链数据接口、区块链应用接口、用户数据、权限管理、链管理等，良好的管理层服务将极大地降低客户的开发难度和业务接入成本。

区块链层实现了多链整合，包括智能合约引擎、跨链引擎、数字资产、共识验证服务、共享账本(分布式账本)、安全隐私保护服务等功能，实现了链间的互联互通。

云平台层则包括云计算服务器、云存储服务器[27-28]等，对主机及容器提供了灵活高效的支持，以此实现跨平台的灵活运行和部署，其中还包括基于高可行硬件服务实现的加密隐私保护服务，如蚂蚁BaaS平台的TEE合约链使用CPU进行密码学隐私保护。

3.2 BaaS技术架构

BaaS技术架构可分为3层：核心层、接口层和应用层。核心层BaaS Core对主机提供了灵活的云资源平台，以实现跨平台部署和运行。使用云服务器在高可靠、保护隐私的可信执行环境下提供智能合约管理、安全隐私防护、浏览器、节点管理、证书秘钥管理、审计日志、链下数据同步、跨平台访问和异构链访问、联盟管理[29]等多种功能，其跨链服务是BaaS平台最新也最为重要的技术支持，实现了数据互通等需求，为用户提供了便捷高效的服务。BaaS平台除本平台区块链外大部分可支持Fabric和Quorum等大型区块链项目。

接口层即包含平台架构中管理层的开发接口和数据接口，除此之外将跨链服务、实名认证、智能合约安全检查、溯源等底层功能封装为标准接口，提供给开发者和用户接入使用，以降低开发者的开发成本和维护成本，便于用户查询数据等；其同时提供了给开发者的智能合约开发接口，实现了BaaS平台的个性定制功能。

应用层即开发者们使用接口层提供的开发接口开发的诸多应用，包括面向非开发者的金融工具、网购应用，还涉及医疗、政务服务和公益等多方面；同时还包括部分开发者设计的面向开发者的实用工具，极大地提高了BaaS平台的可用性和拓展性。

BaaS平台的技术架构如图4所示。

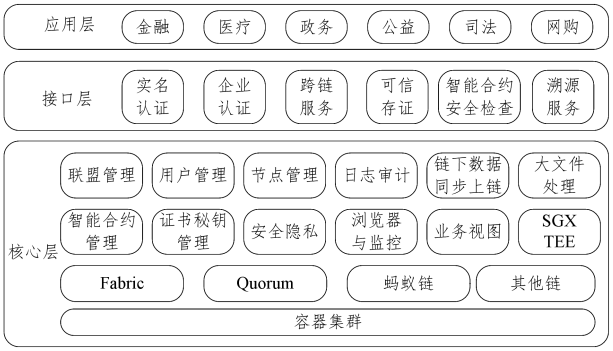

图4 BaaS平台的技术架构图

Fig. 4 BaaS technology architecture

4 当前应用现状分析

4.1 BaaS云服务平台

(1)Oracle Blockchain Platform

Oralce推出的区块链云集成生态主要面向Oracle数据库的防篡改区块链表，支持语义操作、数据服务、区块链云服务等，结合基础设施云服务(Infrastructure as a Service，IaaS)[30-31]、平台服务(Platform as a Service，PaaS)[32-33]和软件服务(Software as a Service，SaaS)[34-35]等云计算服务。

BaaS的使用技术流程为用户通过基于Fabric的SDK接口接入BaaS，并通过TLS协议[36-37]数字签名进行登记，系统内成员服务容器认证授权，请求身份管理云服务，身份管理云服务器确认身份后向用户发送登记证书；用户随后向节点容器请求背书，由背书节点向智能合约容器请求智能合约代码后节点向用户发送已签名RWset；此时用户可以提交已背书签名的交易至共识容器，共识容器内节点负责批量打包交易，其包括对象存储云服务和基于Kafka[38-39]的EventHub云服务，再将交易包发送至节点容器内的提交节点，提交节点负责将交易写入区块并更新账本状态；最后节点容器将事务已经提交的通知发送至用户，该事务即完成。图5为Oracle Blockchain Platform的基本架构图。

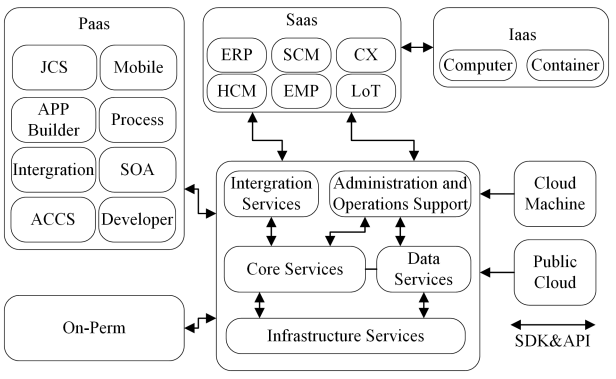

图5 Oracle Blockchain Platform基本架构

Fig. 5 Oracle Blockchain Platform architecture

(2)Azure

微软的Azure区块链是基于联盟区块链[40]开发的，使用严格的邀请准入制度，仅获得许可的联盟成员才有执行智能合约的权限，Azure提供的BaaS服务较好地保护了数据隐私和链上安全，以便于成员内部的运营管理和互操作。

Azure中间件与公有链BaaS平台有所不同，其活动目录和私钥库涵盖了身份验证、授权、私钥发放、存储访问和生命周期管理功能，上述功能为Azure提供了严格的准入机制和链上安全性；区别于公有链上的透明性，联盟链需要保证链上数据的隐私性，因此提供加密服务，保证链上交易数据只能由交易参与者查看；使用基于Interledger[41-42]的跨链分布式分类账方法保证生态内账本的一致性，且提供公钥为监管者和使用者进行数据服务。

Azure使用网络隔离技术[43]，事务和验证节点都是一个虚拟机，不同网络的虚拟机之间无法直接通信，进而保证生态内服务的安全性。

(3)TBaaS

腾讯云区块链服务(Tencent Blockchain as a Service，TBaaS)，是基于联盟链开发的，主要针对金融应用场景，接入Hyperledger，TrustSQL，BCOS，Corda，EEA等系统生态，提供了大数据分析、云安全、自动化运维[44]、人工智能[45]等多种服务，其源代码已开源至Linux社区，可实现跨链访问、硬件加密等。TBaaS使用Kubernetes[46]集群进行联盟链监管服务，包括平台数据监控、人工智能数据分析、故障警报、数据报表生成等。

(4)Antchain BaaS

蚂蚁链区块链云服务平台(Antchain BaaS)，是基于蚂蚁区块链平台开发的，可部署于金融、医疗、工业互联网、政务、公益等多种应用场景，其优势在于简单易用、部署灵活、可实现定制。图6为Antchain BaaS技术架构图[47]。

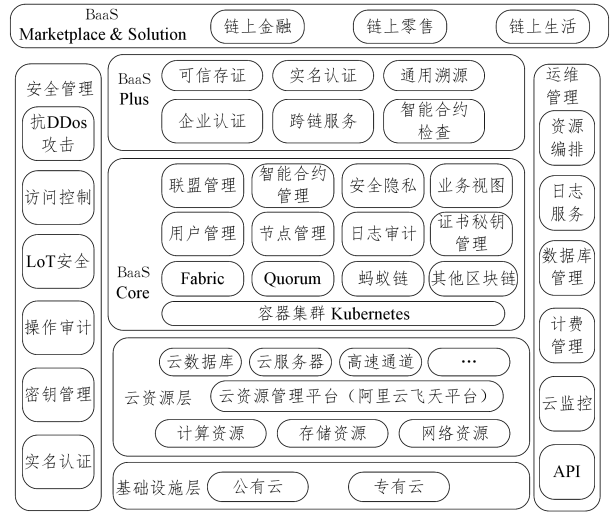

图6 Antchain BaaS技术架构图

Fig. 6 Antchain BaaS architecture

Antchain BaaS是一个大型区块链开放式云平台，提供了高效安全的跨链服务和加密智能合约服务，保证了用户的业务安全，同时其存证平台、合约平台、跨链平台等均使用蚂蚁自研的高隔离性虚拟机支撑，进一步提高了系统的业务安全性。

Antchain BaaS 除支持蚂蚁链外，还支持 Fabric、Quorum、比特链、以太链等多种异构区块链，良好的跨链服务保证了交易可快速上链。其跨链服务包括账本数据访问和合约消息推送两类服务及其对应的 API 接口。账本数据访问可以帮助用户智能合约获取其他区块链账本上的数据，包括区块头、完整区块、交易等数据。合约消息推送服务可以帮助部署了跨链数据服务的不同区块链上的智能合约进行消息通信，满足跨链业务关联处理等场景。

表 1 列出了上述云服务平台的优缺点及技术亮点。

表 1 云服务平台的对比

Table 1 Comparison of BaaS

BaaS 平台	Oracle Blockchain Platform	Azure	Tencent BaaS	Antchain BaaS
适配链	Fabric	Azurechain	FabricBcos	Antchain FabricBCOS
共识机制	RAFT	IBFTQuorum	Kafka PBFT RAFT	PBFT HoneyBadgerBFT
支持第三方证书	是	否	否	是
隐私保护亮点	无	虚拟网络隔离	无	TEE 硬件隐私合约链

4.2 BaaS 应用场景

基于区块链技术的不可篡改性、可追溯性以及 BaaS 平台的隔离性、灵活部署等多种特性，BaaS 平台可适用于溯源、金融、医疗、工业互联网、政务、公益等多种应用场景。

(1)跨境转账

跨境转账场景涉及银行、金融监管规则、客户端服务器、汇率等多方面因素，导致跨境转账效率极低，且手续费高昂，即使当前部分跨境转账已涉及区块链技术，但是受到共识协议等多种因素的限制，仍然需要等待较长时间，而基于区块链技术的 BaaS 平台可通过云服务建立链上跨境汇款通道，通过智能合约及金融联盟链协议和监管，降低转账成本并大幅提高转账处理效率。

(2)商品溯源

基于区块链数据的不可篡改性，部分商品通过区块链技术实现了产品的溯源追踪，但高昂的开发成本和维护难度限制了大量商品实现溯源，而 BaaS 平台以低廉的服务费用、极低的技术门槛和高效可靠的性能提供了大规模产品的溯源服务，如有机农产品可追溯至其生产、运输、销售、再运输的过程，仍以蚂蚁 BaaS 平台为例，蚂蚁 BaaS 平台 2018 年的双 11 购物节为 1.5 亿件商品提供了溯源服务，蚂蚁 BaaS 平台以其优秀的事务处理速度配合云服务技术实现了大规模的产品溯源，仅区块链技术不可能提供如此庞大的事务处理能力。使用区块链溯源还可以杜绝商品造假、贴牌等可能，根据区块链不可篡改的特性，避免了通过中心化数据库记录被篡改的可能，保证了市场环境的纯净性与可信性。

(3)电子病历

传统电子病历仅通过中心化数据库实现，几家甚至单个医院难以实现数据互通，跨医院、跨城市的转院患者需要重新检查，耽误救治时间，浪费医疗资源，而基于 BaaS 的电子病历可在保护患者隐私的基础上，上链患者病历信息，实现全网络的信息互通，便于患者诊疗。由于信息的不可篡改性，还可以通过电子病历实现医疗保险的便捷报销，同时可根据电子病历的情况解决医患纠纷。

(4)慈善捐款

当前公众对慈善项目的态度往往存疑，诈捐、骗捐等现象层出不穷，基于 BaaS 平台的慈善捐款项目可以在保证隐私的情况下基于联盟链监管机制验证证明信息、证明人情况等，基于区块链的不可篡改和数据透明性由公众监督钱款资金的流向，还可结合电子病历等方式与医疗慈善捐款等项目，实现生态内的交互。

(5)司法存证

司法可信存证是 BaaS 平台非常值得深入的方向之一，链上司法存证可保证司法证据不可篡改，隔离司法系统内部司法取证、司法检验与司法审理，大幅度增强司法正义与司法公平性。而且 BaaS 平台进一步落地拓展后，大量用户可直接将版权专利信息、电子合同、各类协议等数据上链，便于司法取证。

5 BaaS 的挑战与展望

对现有 BaaS 平台进行研究与分析后发现，当前 BaaS 仍受区块链性能瓶颈效应、技术落地性差、缺乏统一标准等问题的限制，随着区块链技术的发展，跨链技术、隐私安全保护等方面的研究越来越多，并在应用中展现了巨大的潜力，但由于区块链技术仍处于起步阶段，仍有许多问题值得深入研究。本文特此提出了关于 BaaS 平台的 3 个应用挑战和 2 个研究展望。

5.1 BaaS 平台面临的挑战

(1)降低操作难度

BaaS 平台的线下使用需要搭建比特币服务端钱包，将链上资金兑换为实体资金，这一技术门槛极大地限制了非技术人员用户对 BaaS 平台的使用，雇佣专业技术人员的成本限制了中小企业及个体经营者对 BaaS 平台的参与程度。如比特币和以太坊的官方钱包对服务端的适配性差，服务端几乎无法使用。因此，当前缺少良好适性的钱包软件内嵌于 BaaS 平台内部。

(2)公有链共识机制

公有链性能受到共识机制发块间隔限制，且 BaaS 平台结合比特链和以太链等价值虚拟货币链实现链上交易，尽管以太坊将发块间隔调整至 15 s，期望的平均交易延迟降至 7 s，但在实际使用中，交易大多在排队，对于追求收益的 BaaS 平台使用高昂的插队手续费是不现实的。在跨链事务中，高延迟会造成链间等待，从而导致多链同时等待，事务无法及时有效地完成，甚至会因为币价波动导致平台或用户承担不必要的损失，过长时延会导致事务撤销并不断重新请求事务，从而造成全系统的等待和瘫痪。

(3)平台间标准化问题

当前 BaaS 平台蓬勃发展，各行业纷纷推出了相关的 BaaS 平台，如金融行业中招商银行旗下的 ABS 区块链平台、地产行业中易居 EBaaS 平台、游戏行业中广州微链 GGC 全球游戏链平台、电商行业中京东智臻链等，大量的 BaaS 平台使用各自制定的标准协议，导致链上账本结构、发块周期、块结构、交易吞吐量等均有所差异，给后续发展过程中平台间的互联互通和兼容性产生了阻碍，难以实现区块链跨平台一体化进程，不利于行业间的融合发展和用户的便捷使用。

5.2 未来研究展望

(1)链间并行

当前大部分 BaaS 平台已实现跨链访问，增强了系统的互操作性，但链间事务并行机制仍未实现，良好的事务划分及链间事务并行机制将进一步提高 BaaS 平台的使用效率，在平台内部可实现多链多共识并借助用户容器共享用户基础，各链并行地处理子事务实现公有区块链扩容，简化系统架构，降低数据处理和维护的压力，并提高系统的安全性。

(2)事务并发量

BaaS 平台基于云服务模式，已显著提高因 Pow 共识机制[48]、PBFT 共识机制[49]和网络带宽限制的吞吐量，但对于庞大的使用需求，公有云节点较多，网络节点跨物理大区的因素限制了广域网上 BaaS 平台的交易吞吐量。

部分平台通过提高区块大小来提升吞吐量导致系统使用量较少时，确认交易时延过长，严重影响了用户的体验感。未来可基于云分发网络[50](cloud-delivery networks)的区块链分发网络[51](blockchain distribution network)来提高系统的整体吞吐量，同时为 BaaS 平台内多种链上货币提供可伸缩性。

在平台内部繁忙时可引入闪电网络实现小规模操作的链下交易，仅将最终结果提交至链上，减少链上的冗余数据，避免系统拥塞。闪电网络在交易双方提供微支付通道，发生交易纠纷后移回平台内链上进行裁决，在保证交易安全性的情况下实现链下扩容，提高 BaaS 平台的吞吐量。由平台内公有云服务器设置的容器记录闪电网络相关交易信息和过程，保证交易的可追溯性。

结束语 规范化的 BaaS 平台已初步实现了区块链技术落地，BaaS 具有的便于开发、易于使用、降低开发成本等优点吸引了越来越多的从业者与区块链用户的使用，如蚂蚁 BaaS 平台将几乎完整的一套区块链前沿技术内嵌至平台，推进了区块链开发使用的规范化和标准化，并提供了多样的应用场景，使得大量商家用户参与到区块链技术的成果分享。BaaS 平台技术仍存在一定问题，如事务并发程度差、吞吐量限制、交易时延较长等问题仍需要 BaaS 平台的开发者解决，但其发展必将为现实世界提供更多的便利，促进区块链技术各个领域不断变革与融合。

参 考 文 献

[1] SATOSHI N. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. https://bitcoin.org/bitcoin.pdf.

[2] BEN Č IĆ F M, ŽARKO I P. Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph[C]// 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). 2018: 1569-1570.

[3] LENG J D, LV X Q, JIANG Y, et al. Consensus Mechanisms of ConsortiumBlockchain: A Survey[J]. Data Analysis and Knowledge Discovery, 2021, 5(1): 56-65.

[4] TAN M S, YANG J, DING L, et al. Review of Consensus Mechanism of Blockchain [J]. Computer Engineering, 2020, 46(12): 1-11.

[5] LONEA H, NAAZ R. Demystifying Cryptography behind Blockchains and a Vision for Post-Quantum Blockchains[C]// 2020 IEEE International Conference for Innovation in Technology (INOCON). 2020: 1-6.

[6] YU G, NIE T Z, LI X H, et al. The Challenge and Prospect of Distributed Data Management Techniques in Blockchain System [J]. Chinese Journal of Computers, 2021, 44(1): 28-54.

[7] SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: Architecture and Research Progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[8] HUA S, ZHANG S, PI B, et al. Reasonableness discussion and analysis for Hyperledger Fabric configuration[C]// 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). 2020: 1-3.

[9] ABUHASHIMA, TANC C. Smart Contract Designs on Blockchain Applications[C]// 2020 IEEE Symposium on Computers and Communications (ISCC). 2020: 1-4.

[10] YANG S, LIU H S, CHENG Y. Overview of design and implementation of cloud computing security system[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2020, 32(5): 816-824.

[11] ZHENG W, ZHENG Z, CHEN X, et al. NutBaaS: A Blockchain-as-a-Service Platform [J]. IEEE Access, 2019, 7: 134422-134433.

[12] XU Z Y, ZHOU X. Survey on crosschain technology[J]. Application Research of Computers, 2021, 38(2): 341-346.

[13] GUO C, GUO S Y, ZHANG S L, et al. Analysis of cross-chain technology of blockchain[J]. Chinese Journal on Internet of Things, 2020, 4(2): 35-48.

[14] ALEKSIEVA V, VALCHANOV H, HULIYAN A. Implementation of Smart-Contract, Based on Hyperledger Fabric Blockchain[C]// 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA). 2020: 1-4.

[15] JIANG Y, LV R Z. Overview of Blockchain Consensus Algorithms[J]. Journal of Jiamusi University (Natural Science Edition), 2021, 39(2): 132-137, 161.

[16] KANG H Y, DENG J. Survey on Blockchain Data Privacy Protection[J]. Journal of Shandong University (Natural Science), 2021, 56(5): 92-110.

[17] JIAO J, KAN S, LINS W, et al. Semantic Understanding of Smart Contracts: Executable Operational Semantics of Solidity [C]// 2020 IEEE Symposium on Security and Privacy (SP). 2020: 1695-1712.

[18] KHANS A, AGGARWALR K, KULKARNI S. Encryption Schemes of Cloud Computing: A Review[C]// 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). 2019: 23-26.

[19] BAO Y H, FU Y J, CHEN W W. Research Progress on Key Technologies of Multi-Cloud Storage[J]. Computer Engineering, 2020, 46(10): 18-32, 40.

[20] ZHANG Z W, WANG G R, XU J L, et al. Survey on Data Management in Blockchain Systems[J]. Journal of Software, 2020, 31(9): 2903-2925.

[21] DAI B R, JIANG S M, LI D W, et al. Evaluation model of cross-chain notary mechanism based on improved PageRank algorithm [J]. Computer Engineering, 2021, 47(2): 26-31.

[22] YE S J, WANG X Y, XU C C, et al. BitXHub: Side-relay Chain Based Heterogeneous Blockchain Interoperable Platform[J]. Computer Science, 2020, 47(6): 294-302.

[23] KALYANI D, SRIDEVI R. Robust distributed key issuing protocol for identity based cryptography[C]// 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2016: 821-825.

[24] SIRIS V A, DIMOPOULOS D, FOTIOU N, et al. IoT Resource Access utilizing Blockchains and Trusted Execution Environments[C]// 2019 Global IoT Summit (GIoTS). 2019: 1-6.

[25] FAN J L, LI X H, NIE T Z, et al. Survey on Smart Contract Based on Blockchain System[J]. Computer Science, 2019, 46(11): 1-10.

[26] TSUTSUMI D, OHMURA I, ABE T, et al. An AES processing system with a compact CPU core for secure communication in embedded systems[C]// TENCON 2012 IEEE Region 10 Conference. 2012: 1-5.

[27] YU H B, CHEN J, ZHANG K. Design of a Secure Cloud Storage Scheme Based on Blockchain[J]. Computer Applications and Software, 2021, 38(4): 64-68.

[28] LI G H. Blockchain-based cloud storage for digital forensics[J]. Network Security Technology & Application, 2021(4): 155-156.

[29] LI D, WONGW E, ZHAO M, et al. Secure Storage and Access for Task-Scheduling Schemes on Consortium Blockchain and Interplanetary File System[C]// 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRSC). 2020: 153-159.

[30] WANG T, CHANG X, LIU B. Performability Analysis for IaaS Cloud Data Center[C]// 2016 17th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT). 2016: 91-94.

[31] KHAJEH-HOSSEINI A, GREENWOOD D, SOMMERVILLE I. Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS[C]// 2010 IEEE 3rd International Conference on Cloud Computing. 2010: 450-457.

[32] WEN Z, LIANG Y, LI G. Design and Implementation of High-availability PaaS Platform Based on Virtualization Platform[C]// 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC). 2020: 1571-1575.

[33] CHENG T L, QING L, ZHOU L, et al. PaaS: A revolution for information technology platforms[C]// 2010 International Conference on Educational and Network Technology. 2010: 346-349.

[34] LIU G. Research on independent SaaS platform[C]// 2010 2nd IEEE International Conference on Information Management and Engineering. 2010: 110-113.

[35] LIU W, ZHANG B, LIU Y, et al. New model of SaaS: SaaS with tenancy agency[C]// 2010 2nd International Conference on Advanced Computer Control. 2010: 463-466.

[36] YAN L, DENG H J, CHEN X. A Survey of Status and Research on TLS Protocol[J]. Network New Media Technology, 2019, 8(1): 1-8, 17.

[37] YU D R, BIAN F, ZHANG B. Improving TLS Protocol Using Identity-Based Double-certificate Mechanism[C]// 2012 International Conference on Industrial Control and Electronics Engineering. 2012: 48-51.

[38] YUAN X C, FU G, BI J Z, et al. Survey on data caching technology of distributed dataflow system[J]. Big Data Research, 2020, 6(3): 101-116.

[39] NGUYENC N, KIM J, HWANG S. KOHA: Building a Kafka-Based Distributed Queue System on the Fly in a Hadoop Cluster [C]// 2016 IEEE 1st International Workshops on Foundations and Applications of Self * Systems (FAS * W). 2016: 48-53.

[40] WANGX, LI J W, CHAI J P. The Research on the Incentive Method of Consortium Blockchain Based on Practical Byzantine Fault Tolerant[C]// 2018 11th International Symposium on Computational Intelligence and Design (ISCID). 2018: 154-156.

[41] NEISSE R, HERNANDEZ-RAMOS J L, MATHEU-GARCIA S N, et al. An Interledger Blockchain Platform for cross-border Management of Cybersecurity Information[J]. IEEE Internet Computing, 2020, 24(3): 19-29.

[42] THOMAS S, SCHARRTZ E. Interledger whitepaper [EB/OL]. https://interledger.org/.

[43] BASTA A, BLENK A, LAI Y. HyperFlex: Demonstrating control-plane isolation for virtual software-defined network[C]// 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). 2015: 1163-1164.

[44] WANG X T. Construction of Cloud DataCenter based on Virtualization Technology and Automated Maintenance Management[J]. Software Engineering, 2020, 23(11): 27-29.

[45] ZHANG T, GAO T, XU P, et al. A Review of AI and AI Intelligence Assessment[C]// 2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2). Wuhan, China, 2020: 3039-3044.

[46] SHAMIM M, BHUIYAN F A, RAHMAN A. XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices[OL]. https://arxiv.org/abs/2006.15275.

[47] ANT Group. Antchain Blockchain as a Service Documentation [EB/OL]. https://antchain.antgroup.com/docs/11/73763.

[48] AOKI Y, KOSHIZUKA N, SEIKE H. Fork Rate-Based Analysis of the Longest Chain Growth Time Interval of a PoW Blockchain[C]// 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019.

[49] SUKHWANI H,MARTINEZ J M,CHANG X,et al. Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)[C]// 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). IEEE,2017.

[50] LIU Y J. Research on Content Placement Optimization in Cloud Content Distribution Network[D]. Jinan: Shandong Normal University,2019.

[51] AIYAR K,HALGAMUGE M N,MOHAMAD A. Probability Distribution Model to Analyze the Trade-off between Scalability and Security of Sharding-Based Blockchain Networks[C]// IEEE Consumer Communications & Networking Conference (IEEE CCNC'21). IEEE,2021.

MAO Han-yu, born in 1998, Ph.D candidate, is a member of China Computer Federation. His main research interests include blockchain technology and distributed system.

YU Ge, born in 1962, professor, Ph.D supervisor, is a member of China Computer Federation. His main research interests include distributed system and big data management.