软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(1):1−19 [doi: 10.13328/j.cnki.jos.005891]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链即服务:下一个云服务前沿*

朱昱锦, 姚建国, 管海兵

(上海市可扩展计算与系统重点实验室(上海交通大学),上海 200240)

通讯作者: 姚建国, E-mail: jianguo.yao@sjtu.edu.cn

摘 要: 区块链的本质是分布式账本.它作为比特币的底层技术日益被熟知,具有去中心化、开放性、自治性、信息不可篡改、匿名性的特点.区块链即服务(blockchain as a service)则是把区块链当作基础设施,并在其上搭建各种满足普通用户需求的应用,向用户提供服务.区块链即服务已成为云计算领域的研究重点.研究了区块链即服务最新的技术发展状况,结合行业研究和企业实践探索,对区块链即服务的架构以及各模块功能进行了概要设计说明,为区块链即服务的发展提供了通用架构模型.另外,分析了结合区块链即服务的云计算相关技术特点,并给出了可能的攻击模型.最后,结合行业区块链即服务的应用,对区块链即服务的技术前景进行了展望.

关键词: 区块链;区块链即服务;云服务

中图法分类号: TP316

中文引用格式: 朱昱锦,姚建国,管海兵.区块链即服务:下一个云服务前沿.软件学报,2020,31(1):1−19. http://www.jos.org.cn/1000-9825/5891.htm

英文引用格式: Zhu YJ, Yao JG, Guan HB. Blockchain as a service: Next generation of cloud services. Ruan Jian Xue Bao/Journal of Software, 2020,31(1):1−19 (in Chinese). http://www.jos.org.cn/1000-9825/5891.htm

Blockchain as a Service: Next Generation of Cloud Services

ZHU Yu-Jin, YAO Jian-Guo, GUAN Hai-Bing

(Shanghai Key Laboratory of Scalable Computing and Systems (Shanghai Jiaotong University), Shanghai 200240, China)

Abstract: Known as the core technology of bitcoin, blockchain is a distributed ledger technology, which is decentralizated, open, tamper-resistant, and autonomous. BaaS (blockchain as a service) takes blockchain as infrastructure and provides many services satisfying the user requirements. BaaS has become the focus of the cloud computing. This study discusses the architecture of BaaS and the preliminary design of each module, referring to the corresponding researches of BaaS and the current related enterprise projects. It is also analyzed that the characteristics of related technologies while integrating cloud computing with BaaS and the possible threat model is given. At last, the future prospects of BaaS are analyzed after investigating the current BaaS applications. In summary, this study aims to provide a full-knowledge and a reference architectural model of BaaS.

Key words: blockchain; blockchain as a service; cloud services

云计算让传统信息行业变得前所未有的便捷.利用云计算所提供的服务,只需要简单的开发工作,便可以完成需要大量研发和运营时间成本的任务.过去几年已经出现了很多云服务架构,典型的应用架构有基础设施即服务(IaaS)、平台即服务(PaaS)、软件即服务(SaaS).用户可以利用 PaaS 方便地在线管理开发应用;可以利用 SaaS 使用网络软件,比本地软件更方便迅捷;利用 IaaS,可以从完善的计算机基础设施获得服务.

近年来,区块链技术在互联网领域飞速发展.它起源于 2008 年,由化名为“中本聪(Satoshi Nakamoto)”的学者

* 基金项目: 国家自然科学基金(61572322, 61772339, 61525204)
Foundation item: National Natural Science Foundation of China (61572322, 61772339, 61525204)
收稿时间: 2017-03-28; 修改时间: 2018-06-20; 采用时间: 2019-09-24; jos 在线出版时间: 2019-11-06
CNKI 网络优先出版: 2019-11-06 11:49:25, http://kns.cnki.net/kcms/detail/11.2560.TP.20191106.1149.011.html

在密码学邮件组发表的奠基性文章《比特币:一种点对点电子现金系统》[1]而展开.区块链是一种按照时间顺序将数据区块以链表的方式组合成特定数据结构,并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账(decentralized shared ledger),能够安全存储简单的、有先后关系的、能在系统内验证的数据.区块链技术具有最普适的底层技术框架,可以为诸如金融、医疗、公共设施领域带来深刻变革.但由于学术研究的相对滞后,区块链技术还远不能达到传统技术的性能.为促进区块链的更快发展,首先需要把这项技术带进工业界和商务领域,而云计算平台则提供了最好的服务传递方式,利用云服务平台的应用可以减少企业区块链开发的大量后端工作.

针对区块链的云服务形态,IBM 和微软正尝试定义一个新的区块链即服务(BaaS)市场.不同于之前的软件即服务、平台即服务与基础设施即服务,区块链即服务是基于区块链向客户提供特定云服务.微软在 2015 年 11 月推出了自己的 BaaS 平台,IBM 也相继在 2016 年 2 月发布了 IBM 区块链服务.同时,微软和 IBM 还各自推行独立的开源项目.IBM 在 2015 年 12 月发起超级账本项目(hyperledger project)[2],微软也在同年 6 月发布 Bletchley 计划[3].可见,未来区块链的发展主要会集中于对 BaaS 的研究,通过云服务基础设施将区块链技术普适化,变革如今的互联网架构.

本文第 1 节概述区块链与区块链即服务的概念和两者之间的关系.第 2 节介绍区块链即服务的典型架构模型,并给出常见的参考架构模型.第 3 节讨论由区块链即服务支撑的云技术特点.第 4 节介绍区块链即服务可能的攻击模型.第 5 节介绍区块链即服务的应用现状.第 6 节展望区块链即服务的未来前景.第 7 节总结本文内容.

1 区块链即服务概述

1.1 区块链

区块链是新型去中心化协议,必须基于分布式系统进行维护.它记录着所有历史交易记录,随着维护节点(矿工)持续生成新区块,数据记录不断增长.所有区块按时间先后顺序组成链式结构,整体架构具有可追溯性和可验证性.利用特定的激励机制,区块链技术保证分布式系统中的节点均会积极参与数据验证过程.同时,系统通过分布式共识算法决定最新的有效区块.另外,区块链技术利用非对称密码学算法对数据进行加密,并通过特殊的共识算法抵御外部攻击,保证了区块链数据的不可篡改和不可伪造.在多方无需相互信任的环境下,区块链利用密码学技术,让分布式系统中所有节点相互协作,共同维护一个可靠的数据日志.

现有的区块链主要分为 3 种:共有链、联盟链、私有链.共有链是完全去中心化的区块链,分布式系统中的所有节点均可参与共识机制和交易,且可以随时加入或退出;联盟链是部分去中心化的区块链,区块链只由特定组织团体维护,预先指派部分节点负责维护共识机制,新的维护节点加入需要提交申请并且通过身份认证,但全网所有节点均可参与交易,查看账本记录;私有链是完全中心化的区块链,维护在特定机构内部,数据的读取权限选择性地对外开放,类似传统大型企业分布式系统,但能提供更强的鲁棒性、稳定性[4].

目前普遍认为区块链技术会经历 3 个发展阶段:以数字货币(如比特币)为主要特征的区块链 1.0 模式;以数字资产和智能合约为核心的区块链 2.0 模式,这一阶段主要触及金融领域,革新传统的债券发行、股权众筹、证券交易;以智能社会为主要特征的区块链 3.0 模式,这一阶段区块链被用于改善社会基础架构,例如身份认证、医疗、域名、签证,被称为“万物互联”的最底层协议.

区块链最初是作为比特币的底层技术而得到关注,但比特币只是区块链的一个实验性产品,区块链还能应用于更加广阔的领域,比如医疗、物联网、供应链、安全认证、社交以及人工智能领域.《经济学人》称区块链为“the Trust Machine(信任的机器)”,因为如今它展现的潜力对于全球金融甚至社会结构都会产生巨大且深远的影响.

1.2 区块链即服务(BaaS)

区块链是去中心化的分布式账本,被用于记录历史交易数据,具有不可篡改、不可伪造、可验证性、可追溯性的技术优势,目前已存在的具体应用包括加密货币(比特币、以太币等)以及智能合约.区块链作为底层分布

式账本技术,可替代如今的数据存储、数据传输系统模块,并作为底层架构向公众提供服务.区块链最大的革新就是支持所有节点能够一同验证和维护数据的有效性、正确性、完整性,从而减少了对中心化节点控制的需要.传统的分布式系统是一个区域性的或者全球化的分布式网络中心,所有主机之间相互信任,并相互协作对全网提供服务.但区块链允许分布式系统中各个节点不再需要相互信任,并且容忍恶意节点的存在,因此,区块链开启了一个允许任何网民参与的全球化的分布式系统结构.

云计算为了有效利用大量计算资源,以共享资源的方式向大众提供服务.传统云计算是在封闭的企业环境下,需要用户无条件信任云服务提供商而得到发展.但如今的互联网结构变得越来越中心化,大型企业控制着网民的所有信息.区块链技术融合云计算,使得人们可以不再依赖于大型企业,每个人都能够参与到分布式系统的管理,维护由自己掌控的基础设施.这个由上千万分散节点组成的分布式系统,其运算能力不输于甚至远高于企业的网络中心运算能力.

在如今数据窃取、数据泄漏越发频繁的社会背景下,用户越来越关注隐私保护.由于传统云服务模式使得用户对自己的数据失去了控制,用户不愿相信云服务提供商能够妥善保护用户数据.大量用户质疑云服务提供商的合法身份,也因此诞生了诸如 CloudVisor[5]、Intel SGX[6]技术,使得云服务提供商的身份可被验证.区块链完全由大众自己运营,所有个体节点的连接能提供云计算所需要的巨大算力,并且网络中不存在中心节点控制,完全可被用于搭建新的云服务模式——区块链即服务(BaaS).

在区块链即服务的模式下,区块链协议被用于维护了基础的完全去中心化的分布式平台,记录在线记录,并且提供不可篡改、不可伪造、可验证性等功能.基于此平台,系统还需要提供各种辅助功能,以帮助系统对外提供各种各样的云服务,比如分布式存储可以帮助持久化记录用户文档,加密算法可以帮助保护用户隐私数据,智能合约机制可以帮助实现各种自动化的认证服务等.区块链即服务模式应该为了满足用户需求,而不断整合功能模块进入系统,在区块链的账本记录之上,提供丰富的云服务.

未来的云服务可以是直接搭建在公有区块链上,PaaS、SaaS 也可以直接搭建在这个公有云服务架构之上,这个模式可以被称为共有链即服务(public BaaS).共有链即服务完全由分布式节点共同维护,不存在主节点,独立节点地位相同,可能会存在特权认证节点对网络进行升级管理,但任何变更历史记录或者网络升级的操作,则交由独立节点投票决定.也就是说,特权节点只负责提议和管理网络升级,当前网络版本内一切操作权利均交由独立节点.区块链网络也可以是私有链或者联盟链.私有链或者联盟链主要应用于企业或者组织内部,通过有限的主机或几个分布式数据中心搭建局部的去中心化区块链.而特定的几个局部区块链同样可以通过特定的协议相互交流同步,从而组成联盟链,这是对传统云计算架构的改善,提高了云服务的可靠性、安全性,但本质上还是通过大型企业提供的网络中心向大众提供指定云服务.这个模式可以被称为私有链即服务(private BaaS).

开发运行在区块链上的分布式应用或者创建一个新的区块链,需要大量手动开发工作以及强大的后台运算能力.区块链即服务可以结合 PaaS,提供包含多种开发者工具的云基础设施平台,使得用户可以更方便地开发区块链应用,极大地减少了开发工作;可以结合 SaaS,使得用户可以直接享受到区块链应用的便捷性、安全性;可以结合 IaaS,给予用户最大的开发空间来设计自己的区块链,云服务只提供区块链的基础架构.目前,IBM、微软都在自己的云服务平台上集成了区块链即服务,丰富自身的云服务架构[7].

区块链即服务模式带来的主要优势在于区块链所带来的防伪溯源的特性,任何记录在区块链上的数据对所有运营节点都是可验证的,并且所有记录的可见性保证了可对历史数据进行追溯,从而保证该网络上所有交易的安全性.此外,区块链即服务变革的是云服务的基础架构,解放了封闭传统的云服务模式,允许大众运营自己的云服务基础设施,并能提供去中心化分布式系统的安全性、可靠性、透明性.

1.3 区块链即服务的系统特性

- 去中心化:系统依靠的是网络上多个参与者的公平约束,没有中心决策者,所以任意每几个节点的权利和义务都是均等的,而且每一个节点都会储存系统上所有数据.即使单个节点被损坏或遭受攻击,系统服务依旧能稳定运行;
- 高可用性:区块链即服务的底层共识算法采用了拜占庭容错(BFT)共识算法,该算法支持节点动态加入

和退出,实现系统的高可用性,保证业务不间断运行;

- 扩展性:区块链即服务系统支持大规模场景下部署和管理的能力,可以快速进行扩展;
- 透明性:区块链上所有记录均是可追溯的、全历史的、防篡改的,并且每一个节点都会储存系统上的全量数据,保证了系统整体的透明性[8].

2 区块链即服务的典型架构模型

2.1 微软Bletchley(私有链即服务)架构[3]

Bletchley 是微软构建的联盟链生态系统架构模型,通过区块链即服务云平台,为企业提供实时的解决方案.该项目的目标是提供区块链即服务,保证服务对于所有平台、合作者和客户来讲都是开放的、灵活的.

Bletchley 对多个区块链机制提供支持,支持智能合约机制或者未花费交易输出(UTXO)机制.基于智能合约机制的区块链包括 Ethereum、Eris,基于 UTXO 机制的区块链包括 Hyperledger.基础平台层提供了区块链的基础架构,包括共识协议、网络、数据存储这 3 部分.Bletchley 结合平台即服务对外提供多种服务,包括:

1) 身份认证服务:可以为个人、组织、关键交易、合同、物品创建身份认证,这个服务可被用于提供纵向服务,比如了解你的客户(KYC)服务、资产注册;
2) 加密服务:有偿加密服务,机密数据只对拥有者和交易方可见;
3) 加密书签服务:当区块链需要与部分外界数据(如时间、市场消息)交互时,就需要加密书签的参与.共有两种加密书签:效用书签、合同书签.效用书签是处理日期、时间记录、加密功能、外部数据访问;合同书签是由智能合约自动地创建,像智能合约一样,也是一个全代理引擎,不需要外界的干涉.加密书签服务使得加密书签能被智能合约或 UTXO 适配器的加密书签代理安全调用;
4) 区块链门服务:该服务允许智能合约或者标记化的物品能够在不同账本系统之间传递.它提供了账本间交易传输的完整性;
5) 数据服务:核心数据服务,包括数据分析、数据存储等;
6) 管理运作服务:企业联盟分布式账本的部署、管理、运作工具.

Bletchley 封装底层区块链技术,在平台即服务之上,又结合软件即服务,基于不同应用场景,提供相应的解决方案,比如加密服务、身份认证服务等.Bletchley 为用户透明地提供安全可靠的服务,能被用于优化具体的不同产业结构(如图 1 所示).

Fig.1 The architecture of Bletchley

图 1 Bletchley 架构图

2.2 IBM Hyperledger架构[2]

Hyperledger 定义了最基础、通用的区块链即服务协议,被设计用于处理企业与企业或者企业与个人之间的交易,也为了可以在同一个网络中满足不同业务需求.Hyperledger 希望提供高度可用的区块链即服务代码,项目代码模块化也非常合理,主要包括 3 部分核心服务模块(如图 2 所示).

1) 区块链服务(blockchain):利用分布式共识协议管理分布式账本,维护一个区块链基础设施,并通过高效的哈希算法维护世界观(world state)副本;
2) 链码服务(chaincode):该服务提供一种安全且轻量级的沙盒运行模式,是运营智能合约的机制,用于在确认节点(validating nodes)之间的沟通服务;
3) 成员权限管理(membership):该服务用于管理节点身份,保护用户隐私,保证网络上的机密性和可审计性.该服务基于公钥基础设施,引入交易认证授权,利用证书对接入节点和客户端能力进行了限制.

在以上基础服务之上,Hyperledger 还提供了应用编程接口(API)、软件开发工具包(SDK)、命令行接口(CLI),方便了开发人员的开发工作.

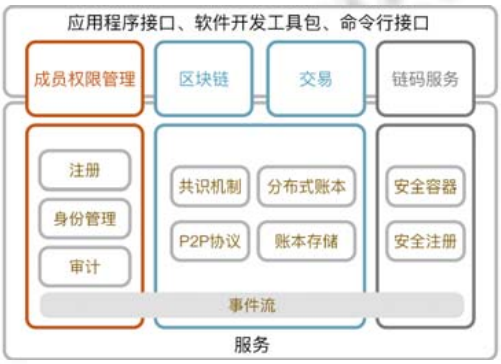

Fig.2 The architecture of Hyperledger

图 2 Hyperledger 架构图

2.3 以太坊架构[9]

以太坊(Ethereum)是一个内置图灵完备编程语言的区块链加密平台,用户能够使用以太坊开发任何功能完备的分布式应用(DApp).以太坊可以用来分散、担保和交易任何事物:投票、域名、众筹、公司管理、知识产权、各种智能资产等.

以太坊的核心部分也是区块链协议,包括共识、点到点(P2P)网络、区块链.区块链负责维护基础的数据记录存储服务,P2P 网络负责节点之间的交互,共识负责保证网络节点状态的一致性.为了支持分布式应用,增强以太坊的平台功能,以太坊还定义了以太坊协议.如图 3 所示,以太坊协议主要包括 3 部分:以太坊智能合约协议、细语(whisper)协议、蜂群(swarm)协议.

1) 以太坊智能合约协议:智能合约是一段由事件驱动的、具有状态的、运行在一个复制的、分享的账本之上的且能够保管帐本上资产的程序.智能合约使得用户可以在区块链上实现自己的逻辑,完成相对复杂的任务.用户、分布式应用发布的智能合约代码与以太坊虚拟机(EVM)进行交互,处理交易事务,同时,通过 RPC 协议进行挖矿和网络事务相关交互,从而实现交易转账等具体商业活动;
2) 细语协议:细语协议是一个通用的点到点通信协议.以太坊的每个节点会为自己生成一个基于公钥的地址,细语协议可以让客户端把信息发给指定的单个或多个公钥地址.节点可以自由地广播有效信息,也可以屏蔽特定的信息;
3) 蜂群协议:蜂群是一个文件存储和传输协议,专门针对静态网页内容的托管.在蜂群里,每一块内容将被存储在 P2P 网络并通过哈希值寻址,这个协议会成为分布式应用程序的骨干.

以太坊从设计的初期就是为建立一个分布式的、智能区块链即服务平台,代替如今所有区块链基础架构,实现安全可信的万物互联网络平台.以太坊的目标就是把区块链特有的安全、开放、去中心化带入几乎所有可计算的领域.如今以太坊已经拥有由 C++、Go、Python、Java 实现的几乎全兼容以太坊协议的客户端,这些客户端可以轻松运行、调试智能合约和 DApp.

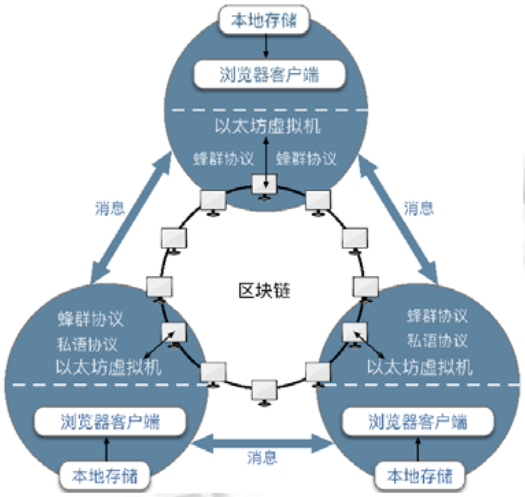

Fig.3 The architecture of Ethereum

图 3 以太坊架构图

2.4 区块链即服务设计架构

我们设计了区块链即服务的通用 3 层架构模型(如图 4 所示):第 1 层是基础设施层,负责数据存储、检索、修改、删除,封装了数据存储的底层细节,对外提供统一的应用程序编程接口(API);第 2 层是中间层,在基础设施之上,扩展了更多协议,使用区块链和分布式文件系统基础架构实现各项点到点的直接通信协议,并且实现了区块链与区块链外界交互信息的相关协议等,进一步拓展了区块链的使用场景;第 3 层是服务层,封装以上所有功能,结合用户需求,抽象出用户需要的相关服务,并提供相应接口支持未来可扩展性,简化用户的开发工作.

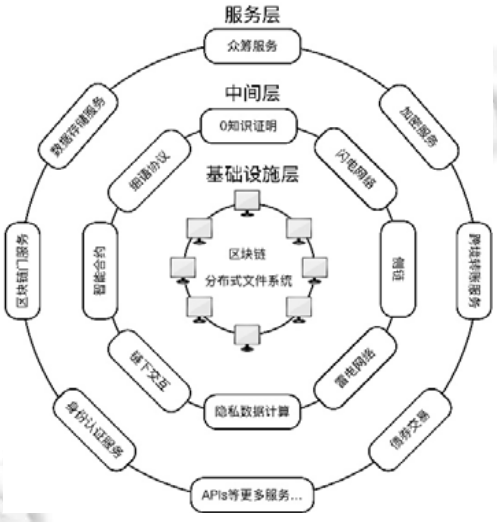

Fig.4 The architecture of BaaS

图 4 区块链即服务架构图

2.4.1 基础设施层

基础设施层是数据层,只关注数据的插入、删除、更新、检索操作.最底层是硬件层,管理专门的硬件设备,可以是真实物理机,也可以是云端的虚拟资源.通过分布式共识算法,普通用户可以使用自己的物理机连接进入公共区块链网络,搭建公有云.同样,企业也可以使用自己的私有服务器搭建私有云.私有云节点数少,便于管理;公有云则更安全、透明,是完全去中心化.区块链和分布式文件系统运行在硬件层之上,具体介绍如下.

1) 区块链:按时间有序地存储系统的所有交易记录,会记录所有操作记录,不可修改,记录可以追溯,公开透明.没有中心节点,所有节点一同参与共识过程,一同做出正确的决策,同步系统状态一致;
2) 分布式文件系统:把大数据切片,分布式地存储在不同节点.当需要获取数据时,首先在区块链的记录中查询文件地址,验证相关权限,再通过点到点协议直接传输文件.这是一个几近无限存储的文件系统,内容发布者也不需要自己保存数据以及维护对外界的服务.

2.4.2 中间层

中间层是扩展协议层,区块链并不是包容万物的技术,如果想应用于更多场景,则需要对其协议进行扩展,包括网络协议、链上链下通信协议,具体包括:

1) 智能合约:智能合约运行在区块链上的一个虚拟机中,当满足内嵌的一定要求时,则可智能地开始执行相关逻辑.这是一个自动状态机,能进一步减少中心化现象,帮助我们实现任何智能协议;
2) 零知识证明(zk-SNARK):零知识证明是对分布式共识算法的补充,可在双方不互相泄漏各自隐私的同时,保证交易的公平进行.因此,通过使用零知识证明机制来隐藏用户的隐私数据,可以在不违反用户隐私安全的同时,保证平台交易的可验证性,从而进一步加强平台的安全性;
3) 侧链协议:一个区块链必然不能满足所有需求,使用侧链协议,则能在主区块链的基础上拓展更符合特定场景的子区块链,复用主链上的电子货币,直接与主链挂钩;
4) 细语协议:这是一个点到点的通信协议,是发布-监听模型.任何节点可以发布自己的主题,其他节点则可以自己选择监听感兴趣的话题;
5) 链下交互协议:区块链运营必然会使用到现实世界中的信息,这就存在可信的区块链与不可信的外部数据如何交互的问题,区块链要能智能识别有效信息,过滤错误的、无效的数据;
6) 蜂群协议:蜂群协议是一个文件存储和传输协议,专门针对网络资源的托管.在蜂群里的每一块内容将被存储在 P2P 网络,并通过其哈希值寻址,目的是为了让任何网络资源可从区块链浏览器上访问到.该协议最终会成为区块链应用程序的骨干;
7) 雷电网络协议:雷电网络是以太坊开发的点到点交易协议,通过智能合约帮助锁定双方资产,需要双方提供证明才能够交易成功,这种链下微支付协议更智能,功能也更强大.

2.4.3 服务层

服务层是用户需求层,企业根据不同用户的需求抽象出具体的服务,包含了数据存储、身份认证、金融交易、API 开发等各种需求,未来这一层也会不断拓展.主要包含以下服务.

1) 软件开发工具包:为进一步定制服务,平台提供软件开发工具包,作为建立应用服务开发工具的集合;
2) 自动化运维服务:利用智能合约可以进行各种运维服务,提供自动审核等功能,从而管理复杂的业务;
3) 跨境转账服务:传统的跨境转账通常需要花费 1~2 天时间,极其不方便,利用区块链即服务的跨境转账服务则能达到实时转账的功能;
4) 云安全服务:区块链即服务是一个去中心化的云平台,免去了被中间商数据扫描的可能性;同时,平台数据经过加密,以保护数据安全.结合定制的漏洞扫描等功能,可以很好地保证云安全;
5) 云存储服务:通过分布式文件系统,为大数据提供数据存储服务,将数据分片,结合点到点直接传输,可以优化数据的存储服务,比单节点存储具有更好的安全性;
6) 供应链自动化服务:区块链即服务可以优化供应链结构,通过减少人为干涉,实现服务一体化、自动化,从而解决供应链管理中的效率低下、及时率和准确性的问题;

7) DevOps 服务:通过区块链即服务,可以搭建一个可部署的 DevOps 生态系统,以替换单一的工具套件,将 DevOps 生态系统以服务的方式输出;
8) 用户权限服务:通过区块链即服务,可以使用访问控制策略来实现对不同用户访问权限的控制,将权限授权返还给用户;
9) 身份管理服务:未来可以把区块链即服务应用于一切物体等身份认证.每个人在出生的时候,或者商品一旦被生产出来,便被分配一个持久的、独特的身份,未来所有活动均会不断更新自己的身份记录信息,并且所有记录都可按时间顺序查询;
10) 大数据分析服务:区块链中数据的不可篡改、全历史的特性以及不断与不同业务场景区块链的数据融合,可以保证区块链即服务收集到庞大的数据集,并提供相应的大数据分析服务;
11) 人工智能服务:区块链即服务可以一方面提供大数据,另一方面提供底层硬件资源,以满足人工智能服务的需要;
12) 应用编程接口:系统给开发人员抽象出一层应用程序编程接口,方便继续拓展功能.

3 区块链即服务支撑云技术

如今,越来越多的服务都迁移到了云端,比如企业资源计划(ERP)服务、海量数据存储、在线编辑工具等.云计算基于互联网,共享大量计算处理资源,完成个人电脑不能承担的任务,提供实时交互服务.云计算提供给企业和普通用户更强的能力来存储、分析自己的数据,保证数据的可靠性、安全性,用户可以真正专注于商业逻辑.专业的云服务可以给业务提供极强的可靠性,良好的架构能够增强系统整体的扩展性、安全性,为数据提供一致性、完整性.

云技术在云计算领域被广泛涉及,云计算主要包括数据、网络、计算、存储这 4 个层面,云存储包含了数据一致性、容错等特性.本节以云技术为出发点,探讨结合区块链即服务技术,把云技术的底层设施从传统网络中心替换为区块链,给云架构带来各个维度的优势.最后讨论区块链即服务的关键技术,阐述提供区块链即服务所需要解决的底层技术难点.

3.1 云计算模式

云计算领域主要涉及到数据、网络、计算、存储这 4 个层面,以下分别进行阐述.

3.1.1 数据层面

- 数据安全:区块链即服务具有原生的安全性、可靠性、可验证性和不可篡改性,让数据能够真正安全地存储、流通.利用内嵌的非对称密码学算法,使得数据能在加密之后,再存储、流通到网络中,同时可在加密的情况下被一般分布式节点验证交易的正确性.结合英格玛(Enigma)[10,11]系统,还能够直接计算加密数据,解决了一直以来必须操作原始数据的依赖性问题,让数据真正变得安全;
- 数据开放:传统云计算追求企业内部数据的隐私性,安全策略也都是保护企业内部隐私数据不可被窃取.如今,随着互联网的不断深入,很多隐私数据(如政府数据、上市公司运营数据等)都被要求向大众公开,走出企业或者政府.然而数据开放的主要难点在于如何在保护个人隐私的同时,安全地开放数据,保证数据传输过程中不会泄漏个人敏感数据.区块链即服务赋予每个人唯一的身份,再结合基于区块链的数据脱敏技术,便能保护数据的私密性,在保护个人隐私的同时,为数据开放提供了解决方案[12].数据脱敏技术主要采用哈希处理等加密算法,英格玛系统[10,11]便能在不访问原数据的情况下对数据进行运算,杜绝数据开放过程中的隐私泄漏问题;
- 数据分析:数据分析是实现数据价值的核心,也是云计算的核心.但在数据分析过程中,需要保护个人或企业隐私,防止核心数据泄漏.传统云计算模式中,需要用户无条件相信云服务提供商,将自己所有的数据以明文形式存放在云端,即便云服务提供商遵守道德,不触碰用户数据,也难以防范云服务提供商的员工出现纰漏.区块链即服务技术可以结合多签名私钥、非对称加密、证书技术,限制数据访问权限.数据被哈希后被统一存储在去中心化的区块链上,只有具有相关权限的个体或部门才能获取到真实

数据,并进行数据分析,或者只是被赋予计算加密数据的权限;

- 数据流通:区块链即服务使得资产能够真正由标记化的数据来代替.由于区块链上的交易记录是可追溯的、永久的、不可篡改的、透明的、全网认可的,所以能够明确记录资产的来源、流通路径、所有权、使用权,对数据流通、资产交易具有很大价值.

一方面,区块链即服务破除了中介复制用户数据的威胁;另一方面,区块链即服务提供了资产可追溯的流通路径,使得一切资产从其诞生开始,就真正做到透明、可追踪,破除了传统云服务商的封闭垄断,允许用户拥有属于自己的数据.Everledger 就是运用区块链即服务技术真实追踪每一颗钻石的来源、流通、买卖,解决了非洲的“血钻”现象[13].

3.1.2 网络层面

传统网络架构是 HTTP 服务的 7 层架构.现今网络上流通的很多数据都是明文,这会导致一种潜在的威胁,用户在获取数据之前,数据可以被黑客截获篡改,导致网络整体安全性存在缺陷.同时,HTTP 服务在过去几十年里已经导致了很强的网络中心化现象,比如中心化的域名系统(DNS)、封闭的大型云服务提供商,变成一个脆弱的、高度集中的、低效的、过度依赖骨干网络的协议.这导致整个网络很容易被监听控制,各国政府可以很容易地监视网络上的一切;同时,中心化的网络结构也很容易遭受 DoS 攻击.整个网络通信传输很低效,过分依赖主节点,主节点的性能成为整个网络的瓶颈.

区块链网络是一个去中心化的分布式网络结构.网络中不存在对主节点的依赖,所有节点对交易处理拥有相同的投票权,是一个完全民主、自治的网络环境.由于网络中不存在中心节点,因此区块链网络更加健壮.

区块链即服务技术派生的分布式文件系统——星际文件系统(IPFS)定义了一种新的互联网架构.传统的 HTTP 服务架构下,当我们访问数据时,需要先到主节点搜索服务器 IP 地址,再通过统一资源定位符(URL)获取对应数据.IPFS 是一个基于内容寻址的文件系统,每个资源都会被分布式地存储在各个节点上,根据资源内容可以分析得到加密哈希名.每个节点的分布式哈希表内存储了部分加密哈希名和存储位置.当用户请求数据时,系统会查询分布式哈希表,在分布式节点之间跳转,从而找到正确的节点.在 1 000 万个节点的网络中,只需要 20 跳便能找到对应的位置[14].IPFS 网络是一个细粒度的、分布式的、异联合的内容分发网络(CDN),可应用于分布式网页服务器、域名系统,还可以结合区块链相关技术,融合加密、认证等技术,保证数据的机密性和安全性,建立身份认证、权限机制.

3.1.3 计算层面

区块链把分布式节点相互连接,组成整个分布式账本系统,作为各种区块链应用的基础设施.现今,比特币使用工作量证明机制(PoW),全网络算力已经达到全球前 500 超级计算机算力总和的 6 000 倍.但比特币中的大量算力都被浪费在挖矿的 SHA256 哈希运算中,并没有用于有效的数据运算[1].以太坊等同样拥有相当庞大的算力.这庞大算力下的区块链,使得整个网络更难被“拜占庭”[15]节点攻击,并且如果能把这算力用于有效的数据运算,则更能体现区块链的优势,革新传统的云计算模式,促进区块链的落地部署.

以太坊内置了图灵完备的编程语言 solidity,理论上能够完成任何算法计算,因此,以太坊可以利用自身的强大算力完成传统企业云所不能计算的难题;同时优化共识算法,减少因为共识所浪费的算力消耗.如今,区块链还不能很好地利用拥有的庞大算力,solidity 编写的智能合约也不能并行、智能地为分布式节点分配计算任务,造成网络上巨大算力的浪费.Bitcoin-NG 等协议已经很好地提高了整个系统的事务处理能力[16],但区块链的事务处理能力还比不上传统的中心节点服务器.

3.1.4 存储层面

区块链即服务中包含两种数据存储技术:区块链服务、星际文件系统(IPFS)服务.

区块链是一个分布式账本,是一种不可篡改的、全历史的、安全的数据库存储技术,该技术类似日志架构文件系统(LFS)[17],可以替代原始的本地数据库.全网节点参与数据运算、交易信息验证,在最新区块达成全网共识后,将最新区块添加到历史记录中.区块链服务可用于事务数据存储,便于对系统历史记录检索,存储大型文件索引,负责管理事务逻辑数据.由于全网需要对区块链上的数据达成共识,因此区块链服务不适合存储多媒体

文件等大型数据文件,需要分布式文件系统作为辅助存储.

传统的云计算系统中广泛使用的分布式文件系统有谷歌文件系统(GFS)[18]和 Hadoop 分布式文件系统(HDFS)[19],但这些传统分布式文件系统仍需要主节点存储所有哈希表,便于到对应分布式节点读取相关文件.主节点的存在引入了可能的瓶颈问题,并造成中心化现象,易于攻击,弱化了整体系统容错能力.区块链即服务应用了星际文件系统(IPFS)[14],这是一个面向全球的、点对点的分布式文件系统.该协议先将内容分片,再分布式地存储到不同分布式节点中,并且应用分布式哈希表(DHT)[20,21]索引文件,消除了主节点的存在必要性,真正做到分布式存储文件.这项服务主要用于存储大型文件内容,比如网页文件、多媒体文件、文档代码等,作为区块链服务的辅助存储服务.

3.2 区块链即服务关键技术

3.2.1 分布式共识算法

在分布式系统中,当多个主机通过异步通信方式组成网络集群,统一对外提供服务时,这种网络默认是不可靠的,任何一台主机都可能出错,我们无法辨别主机或网络性能降低是否与主机宕机相关,也就是说,我们无法观察到实际错误[22].为了保证服务的持久性、正确性、一致性,则需要在这些不可靠的主机之间复制状态,以保证每个主机的状态取得共识.区块链由于对分布式系统的依赖,也不可避免地需要共识算法保证系统状态的一致性.

共识算法分为有领导人(leadership)共识算法和无领导人(leaderless)共识算法.常见的两种故障模型包括故障-停止模型和拜占庭模型,前者只考虑机器自身可能出现的停止服务情况,后者还会考虑恶意节点存在的情况.恶意节点存在恶意行为,会主动、刻意地危害系统安全.

有领导人共识算法能够在问题发生时进行复杂的强协调处理,通常提供很高的事务处理效率.但在保证可靠性的同时,有领导人共识算法也聚集了单点风险,而且选取领导人的过程也是对算力的浪费.此类算法包括 Raft[23]、VRR[24]、MultiPaxos[25]、FastPaxos[26]等.因为领导人的恶意行为无法被检测,通常只能容忍故障-停止模型.区块链是一个全网分布式系统,不可避免地会存在恶意节点,因此这类算法不适用于区块链技术.

无领导人共识算法仅通过投票判断决策的正确性,没有领导人或协调者的介入,通常需要更多的通信时间才能达成共识.这种算法具有更强的容错能力,通常用于解决“拜占庭问题”[15],包括 Basic Paxos[27]、Egalitarian Paxos[28]、PBFT[29]、PoW[1]、PoS[30]等.由于整体的无主结构,系统也更加安全,单节点的行为不会影响系统表现,同时防范了 DoS 攻击.现在,不同的区块链技术会根据自身业务需求选择合适的共识算法,比如:PoW 算法需要全网 50%算力才可发动有效攻击,但共识时间过长;PoS 缩短了共识时间,但可能会导致系统受到拥有大量投票权的单个节点控制;Ouroboros 重新定位 PoS 内的安全问题,给出了更加安全的、更高效的 PoS 共识算法[31].Proof of Luck[32]结合 Intel SGX,利用可信执行环境(TEE),为区块链的节点提高更加安全的执行环境,进一步提高了区块链的安全性.

当使用区块链共识算法时,需要考虑共识过程中可能出现的两种情况:矿工没有动力挖矿、矿工挖到矿后不广播给其他节点[33].对于这些现象,我们可以利用不同的激励机制以及算法改进来保证矿工遵循协议正确运行,惩罚错误行为,保证正确节点利益最大化[1,16,33].

3.2.2 侧 链

分布式共识算法是区块链的核心,侧链技术是实现区块链网络价值的关键,是区块链与外界通信和扩展服务的纽带.

比特币作为区块链技术、电子货币的鼻祖,自然会获得最多的关注和拥护.本身局限的使用范围,使得比特币很难扩展到其他应用场景,目前仅局限于电子货币支付.锚定侧链技术[34]的提出,使得数字资产能够在不同区块链上传输,允许人们在现有的电子货币框架上创新应用场景更范式的区块链系统.通过将新的电子货币与比特币等高价值电子货币挂钩,可以解决新货币流通不足、市场价格波动大的问题,从而保证新货币的认可度.同时,主链与侧链是相互独立的,一个恶意的侧链并不能影响到主链.

3.2.3 智能合约

智能合约是一段运行在区块链上的程序代码,可以智能地运行在区块链服务上,在满足限制条件后,自动执行合约.一个智能合约包括程序代码、存储文件和一个账户余额.任何用户都能发布一个交易来创建智能合约,程序代码在智能合约创建后便不能再被修改.如果用于实现智能合约的编程语言被证明是图灵完备的,这意味着智能合约可被用于解决所有计算问题,也便能像云计算服务模式一样,向公众提供各种各样的云服务.以太坊的智能合约机制支持图灵完备的 solidity 语言.

智能合约的推出,减少了对可信第三方的依赖,同时减少了用户的参与度,允许智能地执行社会任务.智能合约还能改善数据流通、安全性,使得用户可以掌控自己的数据.由于程序代码的高效性,智能合约可以改进如今的金融、政府等诸多架构,极大地提高了社会工作效率,增强社会的公信度,减少金融欺诈的可能性,最终实现一个在规章制度下自制的社会.

如今已经存在一些完备的智能合约体系,比如 Hawk[35].但智能合约的核心只是一段程序代码,不可避免地会存在缺陷,比如调用未知者(call tothe unknown)、异常混乱(exception disorder)等.攻击者则可以使用这些特性对区块链发动攻击,比如以太坊的 DAO 攻击[36].未来智能合约还需要优化自身设计,提高区块链整体的安全性,以太坊 DAO 攻击事件是一个警示.

3.2.4 分布式文件系统

传统的文件系统都是单节点存储,或者是单个网络集群内部的分布式文件系统,如 Hadoop 分布式文件系统(HDFS)[19]和谷歌文件系统(GFS)[18],不同个人、企业各自保管自己的文件.为了满足全球化文件共享,全球化分布式文件系统概念被提了出来.

如今,很多点到点(P2P)文件共享应用取得了成功,比如迅雷、BitTorrent、Napster 等.这些文件分布式系统同时支持上百万用户在线共享文件,但是还没有一个分布式系统能够满足全球化的、低延时的、去中心化的要求.HTTP 协议是最成功的“文件分布式系统”,利用互联网将成千上万的独立文件连接在一起.但 HTTP 协议并不是一个完全的去中心化分布式系统,是一个多中心化的文件系统.如今,我们步入去中心化、自治的新社会发展形态,数据分布式存储具有了新的挑战.

1) 分布式存储巨量的数据集;
2) 跨组织、地域完成计算;
3) 高清实时的视频流;
4) 巨量数据集的版本控制;
5) 防止重要文件的意外丢失.

这些特性都是如今 HTTP 协议所不能提供的.区块链即服务框架下给出了一种新的分布式文件系统:星际文件系统(IPFS).所有文件被分布式存储在全网,通过单个节点的分布式哈希表提供文件地址查询,再直接点对点传输文件;同时,可以运用多节点并行下载加速数据传输速度.由于近似无限的个人节点,存储空间可以看作是无限的,因此重要数据、大数据集都可以多加备份.IPFS 为我们定义了全新的基于内容的分布式互联网架构,在这个系统中,没有中心化节点控制,获取内容是完全可靠、可信的,陈旧但是重要的文件不会丢失,信息发布者也不需要强制管理自己的内容,可以由对相关内容感兴趣的个人节点负责存储[14].IPFS 能给我们一个可信的、扁平化的、永久存储的互联网.

3.2.5 区块链扩容技术

评估区块链即服务的一个重要的指标是系统的吞吐量,即系统每秒可以处理的交易量.这个指标限制了系统的规模和发展的潜力.从技术角度来看,所有区块链的共识协议都有一个具有挑战性的限制:网络中的每一个完全参与的节点都必须要验证每一笔交易,并且这些节点必须和它的其他节点保持一致,这是区块链技术的组成部分,它通过创建分布式的账本来保证区块链的安全.扩容技术可以有效地解决这个问题,如今主要存在的扩容技术如下.

- 分片技术[37].分片技术是一种基于数据库分片传统概念的扩容技术,它将数据库分割成多个碎片,并将

这些碎片放置在不同的服务器上.在公共区块链的环境中,网络上的交易将被分成不同的碎片,其由网络上的不同节点组成.因此,每个节点只需处理一小部分传入的交易,并且通过与网络上的其他节点并行处理就能完成大量的验证工作.将网络分割为碎片会使得更多的交易同时被处理和验证.因此,随着网络的增长,用区块链处理越来越多的交易将成为可能;

- 分级设计.区别于分片技术,将网络划分成不同的区域,分级设计尝试把主要的交易发送给主链,而把小额的、零碎的交易发往链下网络(雷电网络[38]).通过使用雷电网络来分流主链的压力,雷电网络中交易的合法性则由交易方的签名保证;
- 共识算法改进.另外,通过改进区块链共识算法,同样可以达到扩容的效果.Bitcoin-NG[16]通过选举临时的主节点(leader)来提高共识达成速度,以此提高了整个系统的事务处理能力.

4 区块链即服务的攻击模型

区块链是一个纯软件实现的分布式系统,没有中心节点,完全由网络内所有矿工维护自治.矿工之间使用分布式共识算法进行决策,保证数据的一致性、准确性.区块链只关注数据的机密性、交易的安全性、记录的有序性和完整性,并且内嵌的分布式系统特性能够抵御对单个节点的攻击.因此,我们主要关注于软件逻辑部分、激励机制等设计相关的错误,以及防范利用系统弱点、漏洞发动的重放、双花等金融方面攻击即可.

区块链即服务为网络安全提供了本质上的解决办法,超越了对端点的保护,如用户身份安全、基础设施保护、交易和通信安全等,即便单节点的失败,也不会影响整个网络的正确性,具有极强的容错性.同时,这种结构能为用户带来服务的透明性和可审计特性,让用户消除猜忌,充分地享受共享服务.区块链即服务使用区块链作为基础架构,在保证基础区块链安全特性的同时,也可以进一步封装,对区块链的安全性、可扩展性做出补充.

4.1 重放攻击

以太坊在 2016 年 7 月由于黑客的 DAO 攻击,决定采用硬分叉取回用户的资金,这导致以太坊同时存在两条链,分别被称为 ETC 链和 ETC 经典链.ETC 链是由以太坊团队硬分叉的官方链,ETC 经典链是硬分叉前的原链,这两个链上的代币分别称作 ETH 和 ETC.这两条链上的地址和私钥生产算法一致,交易格式也完全相同,导致在其中一条链上的交易在另一条链上也可能是完全合法的.因此,若在一条链上发起的交易,去另一条链上重放,也可能完全合法,这就是区块链上的“重放攻击”.

以太坊社区如今包容两条链同时存在,且两条链相互独立,链上的资金也相互独立.硬分叉后,在硬分叉前拥有以太币的用户平白多拥有了一份资产 ETC.假设地址 A 在 ETC 链上转账了 100ETH,那么任何人都可以在 ETC 经典链上重放相同的转账交易 100ETC,这种做法完全合法.但地址 A 的用户却在未知情况下丢失了 100ETC 的资产.

若区块链只存在一条链,如今的公式算法以及区块链相关机制可以保证不会存在这种攻击方式,原因是所有记录是有序的、可追溯到的.另外,比特币的未花费交易输出(UTXO)也可天生免疫该攻击,当一个未花费交易输出被使用后,网络中便不再存在此输出,同一笔交易也便不可被重放.

4.2 “51%”攻击

在一个分布式系统中,当攻击者控制超过 50%的节点加入系统时,通过绝大多数投票权发起攻击,恶意节点企图获取整个系统的控制权,这便造成了“51%”攻击.区块链是一个完全去中心化的分布式系统,由网络中的所有节点统一投票,并且根据共识算法判断决策的可信性.完全去中心化的分布式系统中,各个节点应该是相互不可信的,节点可以是出错的,也可以是一个恶意的攻击节点,那么想要在这种环境下进行正确决策,就必须解决拜占庭容错问题,也就是分布式共识算法主要需要解决的问题.该攻击虽然危害巨大,但实施者会很少,除了攻击难度较高外,更主要的原因是这类攻击会直接导致该区块链共识受损、信用崩盘.正常来说,考虑拜占庭问题的分布式系统能够容忍拥有 33.3%算力的恶意节点攻击.

4.3 双花攻击(double spending)

当同一笔收入被花费了两次时,被称作双花.这种攻击方式被称作双花攻击.传统纸币由于是实体物质,实体物质不可复制,只存在一份原本,自然可以抵制双花攻击.区块链中存储的是数字资产,如果不仔细管理控制,很可能会被攻击者利用,套取利润.

在比特币中,是允许同时存在主链和支链的,由于未花费交易输出(UTXO)的特性,单条链中一定不会存在双花的情况.但由于区块链中会存在地域隔离和网络延迟,支链不可避免地会出现,支链中的交易最终会被作废,若支链中交易的商家提前确认了交易,则会造成双花问题,买方平白得到一份资产.所以一般区块链都会鼓励在几个区块产生之后再确认交易,防止由于某条支链的作废而导致已交易资产的丢失.比特币要求交易成功后,再等待 6 个区块的产生,以确保交易的不可逆转性[39].

若某个攻击者控制了 51%的算力,则可以随意控制某个支链在几个区块后成为了主链.此时,主链中的交易被作废,但是商家已经交易了货品,则意味着买家未花费任何比特币,却得到了对应的商品.一般来说,区块链并不能抵御 50%以上算力的攻击,但如今各大矿池都会避免自身算力的大幅上升,单个矿池算力会维持在全网算力 40%以下.

4.4 “自私挖矿”攻击

当旷工成功挖到一个区块后,为了获得更大的收益,而不再有动力把该区块广播给其他节点,便会造成“自私挖矿”攻击.为了解决这个问题,需要考虑到矿工正确挖矿的激励机制,比如矿工有动力去挖矿或者矿工有动力把区块广播给其他节点.为了使得比特币系统抵御“自私挖矿”攻击,Eyal 等人研究了可能容忍的恶意节点的算力总量[40],并给出以下公式:

$$\frac{1-\gamma}{3-2\cdot\gamma}<\alpha<\frac{1}{2}.$$

γ表示矿池所容纳的算力总量占据全网总算力的比例,α表示“自私挖矿”的恶意节点的算力总量占据全网总算力的比例.但是,在网络链路不稳定的情况下,比特币系统并不能抵御拥有全网 23.2%算力的攻击者进行“自私挖矿”攻击[33].Bitcoin-NG 提出了一种新的比特币的模型,使得比特币网络能够容忍 29%的算力攻击,并且提高了整体网络的性能[16].

4.5 网络攻击

4.5.1 数据操纵和欺诈

传统 HTTP 网络中,不可避免地会传输一些明文数据用于显示,这会导致用户在获取数据前,数据可能会受到篡改,或者数据在存储前也可能就受到了篡改.这便导致了数据操纵、欺诈的风险.区块链的主要特点包括不可篡改性,任何节点都不可能单方面改变区块链上的数据.用户的交易数据也会用公钥进行加密,用于维护数据传输的完整性.区块链技术可以保护互联网 BGP 和 DNS 基础设施,防止数据篡改,结合多签名机制,可进一步增强系统安全性[41].无钥签名基础设施(KSI)[42]可以用于加密用户数据,用户不再需要保存自己的私钥,进一步增强了整体网络的安全性.由于区块链内单节点的不可控,因此需要相关的利益刺激以及数据验证技术,保证交易数据的可靠性、正确性.

4.5.2 分布式拒绝服务攻击(DDoS)

2016 年 10 月 21 日,美国 DNS 服务提供商 Dyn 服务器遭受到大规模 DDoS 攻击,导致大量网站不可被访问.这警示我们,脆弱的网络骨干会影响到整个网络的服务性能.由于有大量的网络审查工作,传统 DNS 系统最致命的弱点是对缓存的依赖.区块链即服务提供了去中心化的网络架构可能,可以使用以太坊结合星际文件系统(IPFS).这种新型的分布式网络架构消除了传统 DNS 冗余,为我们提供一个可信、免审查的网络.虽然区块链理论上不可受到 DoS 攻击,但也可能存在一些软件缺陷,从而被黑客利用,危害整个系统,如比特币 0.8.x 版本的系统缺陷 CVE-2013-4627[43].

4.5.3 不可信环境中的数据偷窃

传统系统中,如果想在一个不可信环境中传输数据,则必须先进行加密.但无论如何,处理数据之前必须先要把密文解密成明文,解密之后,明文则很可能会被窃取.Engima[11]使用了多方计算(MPC)[10,44],这是一种加密数据运算技术.多个互不信任机构的合作过程中,这种技术允许在保管自身隐私的情况下完成加密数据的计算,使得计算不再需要依赖于明文.同时,区块链技术会记录带有时间戳的交易记录和文件哈希,数据无法被篡改、删除,也阻止了攻击者隐藏操作行踪.但区块链上,一切数据都是公开的,任何人都可以访问,因此存在数据偷窃的可能.Zerocash[45]指出,可以在保护个人隐私的前提下进行匿名交易.

5 区块链即服务的典型应用

5.1 跨境转账平台——Ripple

Ripple 主要致力于使用区块链即服务技术,实现跨国界和银行间的商务支付平台.作为第一个全球开放的支付网络,允许我们随时随地转账任意一种货币,包括美元、欧元、人民币等,转账不区分国界和银行,简易便捷,交易确认在几秒内完成,且费用几乎可以忽略不计.

使用区块链即服务技术,银行能够很容易实现新的跨境转账功能,以极少的成本将原先以天为单位的跨境转账效率提高到秒级,并且企业开销也削减至微毫.同时,银行也不再需要保存所有的转账文本,所有记录都是可查询的,客户能够自己随时随地查询.银行能够提供一周 24×7 小时的、实时的、信息完整透明的服务质量.Ripple 真正做到了变革传统跨境转账服务.

全球每年跨境转账的额度在 24 万亿,如今 Ripple 还不能支持如此大量的交易.但未来,Ripple 平台会随着技术的不断推广而得到优化、发展.对于我们来说,当下已经是正确的时间来拥抱一个全球化、24 小时、低费用、无延迟的银行转账平台了[46].

5.2 匿名支付平台——Zerocash

比特币本身并不是匿名的,每一笔交易都会直接联系两个地址,由于区块链记录的完整性,最终任何人的交易记录都可以被查询,比特币并不能提供传统支付系统的用户隐私性.Zerocash 是分布式的、开源加密货币,能为交易提供隐私性和可选的透明性.通过给比特币添加加密协议,Zerocash 能够隐藏交易的发送方、接收方、交易金额.用户对自己的交易有完全的控制,能够选择性地向其他人提供观看内容的权限.

由于比特币需要验证交易金额等信息来保证交易的有效性,但 Zerocash 为保护个人隐私,隐藏了这部分信息.因此,Zerocash 提出零知识证明机制(zk-SNARK),这个机制能够保证用户之间没有欺骗或者偷窃,保证了交易的机密性和正确性.最终,Zerocash 能够把比特币的交易花费减少 97.7%,交易确认时间缩短 98.6%,支持匿名支付,并且支付不需要用户参与,可以直接发给指定地址[45].

5.3 分布式域名系统——Blockstack

Blockstack 项目基于比特币,在其上封装了一层“不可知的”域名系统.与传统域名系统类似,Blockstack 允许用户查找、更新、转移、管理域名信息.但 Blockstack 运行在完全分布式的基础设施之上,网络更加透明,减少了政府审查的影响.同时,由于不再存在中心节点缓存,从本质上解决了缓存投毒攻击(cache poisoning).并且,所有域名被加密存储在区块链上,只有拥有对应密钥的个人节点才能控制该域名[47].

基于该域名系统,Blockstack 还推出了 Blockstack 浏览器,希望能够直接搭建一个分布式互联网环境.这个网络中,所有资源被分布式存储在不同节点,用户可以在自己的设备上提供资源访问服务,其他用户则通过 Blockstack 浏览器获取资源地址信息,资源获取过程中不存在任何中间商、密码、数据孤岛等.同时,Blockstack 还提供了统一的 API 文件“blockstack.js”,使得 Blockstack 浏览器的应用开发者不再需要关心维护数据库、运行服务器、用户管理系统相关开发,数据存储过程中也可以提供身份认证机制.如今,Blockstack 应用的存储仓库可以选择 Dropbox、微软 Azure、Google Drive 等.

这一项变革了传统域名系统,解决了互联网越来越中心化的问题,在比特币的基础上,维护去中心化的域名

系统,让网络更加透明、安全、高效、可靠.这一项目是我们逐渐步入自由、民主社会的体现,在不同行业都存在中心化现象的社会环境下,相信区块链即服务技术能够给我们带来更多的传统产业变革.

5.4 存证型应用——Factom

Factom 是利用比特币的区块链技术来革新商业社会和政府部门的数据管理和数据记录的方式,维护了一个永久不可更改的、基于时间戳记录的区块链数据网络,大大减少了进行独立审计、管理真实记录和遵守政府监管条例的成本和难度.Factom 通过建立一个通用数据层,允许用户为自己的数据创建一个独立的虚拟区块链,用户的单个数据包被记为一个输入条目(entry),用户只要把数据输入其中便被及时记录下来,整个过程是分布式的,系统上任何不良行为都会被用户投票系统甄别出来并剔除出去,这是一个完全的共识系统.

Factom 通过允许基于区块链技术来创造新的分类总账,引入了有数学法则保证的分类账本技术的诚实性和不可欺诈的特点,从而把区块链技术的好处和优势带到现实世界中.建立在 Factom 基础之上的应用程序寻求能够直接利用区块链实现追踪资产和实现合约,在自己的架构中记录条目而不用将交易记录写入区块链.与以太坊类似,Factom 系统会创造一个叫作 Factoids 的电子币,持有 Factoids 意味着有权使用 Factom 系统,只要把 Factoids 转化成输入积分,便有权把数据写入 Factom 系统中.同时,运行着 Factom 的联邦服务器也能收获 Factoids 作为维护系统的回报.Factom 虽然同样基于比特币网络,但却并不是之前提到侧链或染色币的技术架构,Factom 只将目录区块的哈希值锚定到比特币区块链,用一种去中心化的方式来收集、打包、安全保护数据[32].

5.5 商品ID管理云平台——VeChain

VeChain 平台是一个基于区块技术的全球账本型信息交互协作云平台.通过 API 与应用层对接,把现实世界中的人、事或物数字化,实现信息的互通互联.通过基于行业实际应用的智能合约,实现不同场景下的协同和价值转移,从而将现实的商业世界映射到区块链上.通过跨平台、跨企业、跨行业、跨国界的互联协作,创造全新的商业模式,为协作参与方提供“信任服务”.

VeChain 源代码的基础主要来源于以太坊,平台上使用的代币为 VEN.VEN 是唯链平台的生态血液,各参与方可以通过支付 VEN 获取相应的产品和服务,主要包括:最终用户付出 ETH 来进行平台的技术开发、商业应用合作的推广、区块链服务的支持;VeChain 基金会通过向智能合约开发服务商收取 VEN,保证各个智能合约的运行,并支付节点奖励给提供商用于平台的日常运行;智能合约服务提供商支付 VEN 获取 GAS 保证合约的运行,并向客户提供服务;应用开发者根据最终客户的需求提供产品,收取 VEN 作为企业收入;最后,最终用户通过支付 VEN 来获取企业产品和服务.

6 未来展望

区块链即服务可以使用区块链技术,改善传统的各个社会领域.所有需要中间人作担保、认证的市场都可以被优化,例如房屋交易、税收征收、债券交易.瑞士银行与英国巴克莱银行正在研究该如何通过区块链加速结算速度,以及 Visa 与 DocuSign 正在研究以区块链技术为核心的汽车租赁验证服务.

微软、IBM、亚马逊已经在区块链即服务领域投入了巨大成本,走在了这个领域的前端.如今,传统云计算企业正在把区块链即服务与现有云架构融合;以太坊也在试图建立一个完全去中心化的区块链应用平台,建立共有区块链即服务.

目前,区块链即服务预计可以在未来给我们带来如下的变革.

1) 金融创新.传统的金融支付、清算、结算,在效率上一直会受到地域的限制,即便互联网已经把世界各地的业务联系在一起,但线下人工操作却会带来不可避免的瓶颈.区块链提供了完全智能化,无需任何人为参与的金融系统可能性[4].比特币解决了超量发行货币、导致金融危机的问题[1];Ripple 则解决了跨境转账效率低下的问题[46];Digix 团队与新加坡金库直接连接,实现了第一个黄金代币,将货币直接与黄金挂钩[48].相信未来区块链能够为我们带来一个智能高效的金融体系;

2) 物联网应用.区块链技术可以把任何电子设备连入到一个区块链网络中,从而使物联网设备能够参与免信交易,智能合约也能够保证执行特定的承诺,使得物联网真正变得智能起来,也为工业界带来更多的商业模式[49].通过基于智能合约的物联网应用,任何数据都可以被交易,未来我们可以真正实现智能城市、智能社会,将共享经济发挥到极致[50,51].Slock 正在建立连接区块链与现实世界的桥梁[52];
3) 优化企业结构.如今的企业都是由最高决策者统一管辖,重大决策也由少数几人确定,但中心化的管理会导致企业运营效率低下,CEO 也很可能会成为企业发展的瓶颈.区块链借鉴蜂巢的思想,提供了去中心管理的可能,依赖于集体智慧做出决策;
4) 追踪供应链.我们生活中会用到各种商品,区块链能够保证商品的来源是完全合法、安全的.在区块链上记录商品的产地、采购、加工、存储等完整流程的真实信息,而且这些信息都是无法篡改的.用户拿到钻石后,便能通过内置 NFC 芯片在 Everledger 查询到开采、物流、门店、海关等完整信息.由于身份证明的唯一性,生产链中任何非法行为都能被检测出来[13].京东也在携手 IBM 研究区块链进行供应链溯源;
5) 互联网去中心化.HTTP 架构下的网络如今已经导致链严重的中心化现象.大型企业控制着云计算资源,用户数据被秘密地在网络上私自倒卖,政府对互联网有着严重的监控,这些现象都与互联网最初的设计理念不符.星际文件系统重新定义了互联网架构,让用户有权限管理自己的数据,实现一个去中心化、点到点的、自由的互联网.域名币则旨在使用区块链技术解决 DNS 服务器中心化的问题[53].未来的互联网应该是公平、公开、公正的;
6) 优化政府结构.Estonia 正在使用区块链技术结合无钥签名基础设施(KSI)[42]帮助运行国内的数字服务,比如电子商务注册服务和电子税收服务,这些服务能够很好地减少政府的管理压力,提高政府工作效率.Estonia 在内的“Digital 5”成员国正在持续研究数字政府的相关技术,并尽量早日落到实处[54].美国华盛顿同样注意到区块链技术[55],中国政府也已经发布了区块链技术发展相关白皮书,相信未来区块链技术一定能够大量应用在政府工作中;
7) 其他.Augur 和 Gnosis 正计划用区块链,结合现实世界的数据可靠地预测市场发展;TransActiveGuild 项目是能源公司 LO3 和 ConsenSys 合作的项目,允许居民自由地转移或者出售剩余的可再生能源给自己的邻居,实现能源转移;婚姻契约同样可以记录在区块上,通过智能合约自动化管理双方资产;选举过程可以使用区块链技术,做到更加透明公正.区块链可以使用的场景还有很多,可用于改善我们生活中无处不见的中心化现象,将社会透明化,实现对智能社会的过渡.

7 总 结

如果说区块链技术是通向未来最具创造性、最有前景的技术,那么区块链即服务便是这个技术中最有效的载体.区块链即服务又可以分为私有区块链即服务和共有区块链即服务.私有区块链即服务搭载在大型企业内部,与传统的云计算平台兼容,提供了更强的数据安全性、可追溯性、不可篡改性以及由于去中心化,而减少了极大的性能瓶颈.共有区块链即服务是最新的云计算架构,由全球网民维护基础架构,云服务提供商使用区块链基础设施继续拓展功能,抽象出上层业务需求,但并不拥有底层区块链基础设施的控制权.

本文研究了主流区块链即服务框架,参考设计了 3 层区块链即服务框架,包括基础设施层、中间层、服务层.本文还探讨了区块链即服务支撑的云技术特色,包括云计算和云存储两方面,深入讨论了区块链即服务的关键技术,并给出可能的攻击模型和相关应用现状.区块链即服务能应用于任何需要去中心化的场景,能提供最普适的基础架构和服务.虽然现今还存在很多技术局限以及安全隐患,但最终区块链即服务将会给予我们一个自治的、可信的、智能化的和谐社会.

References:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf
[2] The Linux Foundation. IBM’s hyperledger project. 2016. https://github.com/hyperledger/fabric

[3] Gray M. Microsoft's bletchley project. 2016. https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley

[4] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016,42(4):481−494 (in Chinese with English abstract). http://www.aas.net.cn/CN/10.16383/j.aas.2016.c160158 [doi: 10.16383/j.aas.2016.c160158]

[5] Zhang F, Chen J, Chen H, *et al*. CloudVisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. In: Proc. of the 23rd ACM Symp. on Operating Systems Principles. 2011. 203−216. [doi: 10.1145/2043556.2043576]

[6] Arnautov S, Trach B, Gregor F, *et al*. SCONE: Secure linux containers with Intel SGX. In: Proc. of the 12th USENIX Symp. on Operating Systems Design and Implementation. 2016.

[7] Malviya H. Reinventing cloud with blockchain. SSRN Electronic Journal, 2016. [doi: 10.2139/ssrn.2885274]

[8] Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):2092−2115 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[9] Buterin V. A next-generation smart contract and decentralized application platform. 2014. https://github.com/ethereum/wiki/wiki/White-Paper

[10] Andrychowicz M, Dziembowski S, Malinowski D, Mazurek L. Secure multiparty computations on bitcoin. Security and Privacy, 2014,59(4):443−458. [doi: 10.1145/2896386]

[11] Zyskind G, Nathan O, Pentland A. Enigma: Decentralized computation platform with guaranteed privacy. arXiv:1506.03471, 2015.

[12] Dong XQ, Guo B, Shen Y, *et al*. An efficient and secure decentralizing data sharing model. Chinese Journal of Computers, 2018,41(5):1021−1036 (in Chinese with English abstract). http://cjc.ict.ac.cn/qwis/view.asp?id=5000

[13] Lomas N. Everledger is using blockchain to combat fraud, starting with diamonds. 2015. https://techcrunch.com/2015/06/29/everledger/

[14] Benet J. IPFS-content addressed, versioned, P2P file system. arXiv Preprint arXiv:1407.3561, 2014.

[15] Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems (TOPLAS), 1982,4(3):382−401. [doi: 10.1145/357172.357176]

[16] Eyal I, Gencer AE, Sirer EG, *et al*. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the 13th USENIX Symp. on Networked Systems Design and Implementation (NSDI 16). 2015. 45−59.

[17] Rosenblum M, Ousterhout JK. The design and implementation of a log-structured file system. ACM Trans. on Computer Systems (TOCS), 1992,10(1):26−52. [doi: 10.1145/146941.146943]

[18] Ghemawat S, Gobioff H, Leung ST. The Google file system. ACM SIGOPS Operating Systems Review, 2003,37(5):29−43. [doi: 10.1145/1165389.945450]

[19] Shvachko K, Kuang H, Radia S, *et al*. The Hadoop distributed file system. In: Proc. of the 26th IEEE Symp. on Mass Storage Systems and Technologies (MSST). 2010. 1−10. [doi: 10.1109/MSST.2010.5496972]

[20] Kaashoek MF, Karger DR. Koorde: A simple degree-optimal distributed hash table. In: Proc. of the Int'l Workshop on Peer-to-peer Systems. Berlin, Heidelberg: Springer-Verlag, 2003. 98−107. [doi: 10.1007/978-3-540-45172-3_9]

[21] Naor M, Wieder U. A simple fault tolerant distributed hash table. In: Proc. of the Int'l Workshop on Peer-to-Peer Systems. Berlin, Heidelberg: Springer-Verlag, 2003. 88−97. [doi: 10.1007/978-3-540-45172-3_8]

[22] Fischer MJ, Lynch NA, Paterson MS. Impossibility of distributed consensus with one faulty process. Journal of the ACM (JACM), 1985,32(2):374−382. [doi: 10.1145/3149.214121]

[23] Ongaro D, Ousterhout JK. In search of an understandable consensus algorithm. In: Proc. of the USENIX Annual Technical Conf. 2014. 305−319.

[24] Liskov B, Cowling J. Viewstamped replication revisited. 2012. http://hdl.handle.net/1721.1/71763

[25] Lamport L. Paxos made simple. ACM Sigact News, 2001,32(4):18−25. [doi: 10.1145/568425.568433]

[26] Lamport L. Fast paxos. Distributed Computing, 2006,19(2):79−103. [doi: 10.1007/s00446-006-0005-x]

[27] De Prisco R, Lampson B, Lynch N. Revisiting the paxos algorithm. In: Proc. of the Int'l Workshop on Distributed Algorithms. Berlin, Heidelberg: Springer-Verlag, 1997. 111−125. [doi: 10.1007/BFb0030679]

[28] Moraru I, Andersen DG, Kaminsky M. There is more consensus in egalitarian parliaments. In: Proc. of the 24th ACM Symp. on Operating Systems Principles. 2013. 358−372. [doi: 10.1145/2517349.2517350]

[29] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. on Computer Systems (TOCS), 2002, 20(4):398−461. [doi: 10.1145/571637.571640]

[30] Kiayias A, Russell A, David B, *et al*. PPcoin: Peer-to-peer crypto-currency with proof-of-stake. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. 2017.

[31] Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Proc. of the Annual Int'l Crvptology Conf. 2017. 357−388.

[32] Milutinovic M, He W, Wu H, Kanwal M. Proof of luck: An efficient blockchain consensus protocol. In: Proc. of the 1st Workshop on System Software for Trusted Execution. 2016. [doi: 10.1 145/3007788.30077901]

[33] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in bitcoin. arXiv Preprint arXiv:1507.06183, 2015.

[34] Back A, Corallo M, Dashjr L, *et al*. Enabling Blockchain Innovations with Pegged Sidechains. 2014. https://www.blockstream.com/sidechains.pdf

[35] Kosba A, Miller A, Shi E, *et al*. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proc. of the Security and Privacy. 2016. 839−858. [doi: 10.1109/SP.2016.55]

[36] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts. Cryptology ePrint Archive: Report, 2016/1007, 2016. https://eprint.iacr.org/2016/1007

[37] Luu L, Zheng CD, Narayanan V, Baweja K. A secure sharding protocol for open blockchains. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. 2016. [doi: 10. 1145/2976749.2978389]

[38] Ethereum. Raiden netwprk. 2018. https://github.com/raiden-network/raiden

[39] Gervais A, Karame GO, Wüst K, *et al*. On the security and performance of proof of work blockchains. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. 2016. 3−16. [doi: 10.1145/2976749.2978341]

[40] Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 2018,61(7):95−102. [doi: 10.1007/978-3-662-45472-528]

[41] Hari A, Lakshman TV. The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet. In: Proc. of the ACM Workshop on Hot Topics in Networks. 2016. 204−210. [doi: 10.1145/3005745.3005771]

[42] Tate J, Clancy TC. Secure and tamper proof code management. In: Proc. of the 2014 Workshop on Cyber Security Analytics, Intelligence and Automation. 2014. 19−24. [doi: 10.1145/2665936.2665940]

[43] Bitcoin. Common vulnerabilities and exposures. 2013. https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures

[44] Goldwasser S. Multi party computations: Past and present. In: Proc. of the 16th Annual ACM Symp. on Principles of Distributed Computing. 1997. 1−6. [doi: 10.1145/259380.259405]

[45] Sasson EB, Chiesa A, Garman C, *et al*. Zerocash: Decentralized anonymous payments from bitcoin. In: Proc. of the Security and Privacy. 2014. 459−474. [doi: 10.1109/SP.2014.36]

[46] Ripple Labs Inc. The journey to real-time cross border commercial payments using distributed ledger technology. 2016. https://ripple.com/wp-content/uploads/2016/07/Accenture_Ripple_CrossBorderPayments.pdf

[47] Ali M, Nelson J, Shea R, *et al*. Blockstack: A global naming and storage system secured by blockchains. In: Proc. of the 2016 USENIX Annual Technical Conf. (USENIX ATC 2016). 2016. 181−194.

[48] Eufemio AC, Chng KC, Djie S. Digix's Whitepaper: The gold standard in crypto-assets. 2016. https://dgx.io/whitepaper.pdf

[49] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of things. IEEE Access, 2016,4:2292−2303. [doi: 10.1109/ACCESS.2016.2566339]

[50] Zhang Y, Wen J. An IoT electric business model based on the protocol of bitcoin. In: Proc. of the Int'l Conf. on Intelligence in Next Generation Networks. 2015. 184−191. [doi: 10.1109/ICIN.2015.7073830]

[51] Hardjono T, Smith N. Cloud-based commissioning of constrained devices using permissioned blockchains. In: Proc. of the ACM Int'l Workshop. 2016. 29−36. [doi: 10.1145/2899007.2899012]

[52] Jentzsch C. Decentralized autonomous organization to automate governance. 2016. https://download.slock.it/public/DAO/WhitePaper.pdf

[53] Kalodner H, Carlsten M, Ellenbogen P, *et al*. An empirical study of namecoin and lessons for decentralized namespace design. In: Proc. of the Workshop on the Economics of Information Security (WEIS). 2015.

[54] Walport M. Distributed ledger technology: Beyond Blockchain. Report, UK Government Office for Science, 2016.

[55] Brainard L. The use of distributed ledger technologies in payment, clearing, and settlement. 2016. https://www.federalreserve.gov/newsevents/speech/brainard20160414a.pdf

附中文参考文献:

[4] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(4):481−494. http://www.aas.net.cn/CN/10.16383/j.aas.2016.c160158 [doi: 10.16383/j.aas.2016.c160158]

[8] 刘敖迪,杜学绘,王娜,李少卓.区块链技术及其在信息安全领域的研究进展.软件学报,2018,29(7):2092−2115. http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[12] 董样千,郭兵,沈艳,等.一种高效安全的去中心化数据共享模型.计算机学报,2018,41(5):1021−1036. http://cjc.ict.ac.cn/qwjs/view.asp?id=5000

朱昱锦(1994－),男,江苏泰州人,博士,主要研究领域为云计算.

管海兵(1971－),男,博士,教授,博士生导师,CCF 杰出会员,主要研究领域为云计算.

姚建国(1981－),男,博士,副教授,博士生导师,CCF 专业会员,主要研究领域为云计算.