浙江大學

题　目 区块链即服务

作者姓名 石崇重

作者学号 22151094

学科专业 电子信息

所在学院 软件学院

摘要

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。

关键词: 区块链;区块链即服务;云服务

引言

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。

第一章 区块链即服务概述

1.1 区块链

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。

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。

1.2 区块链即服务(BaaS)

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。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。

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)。

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。

第二章区块链即服务的典型架构模型

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.

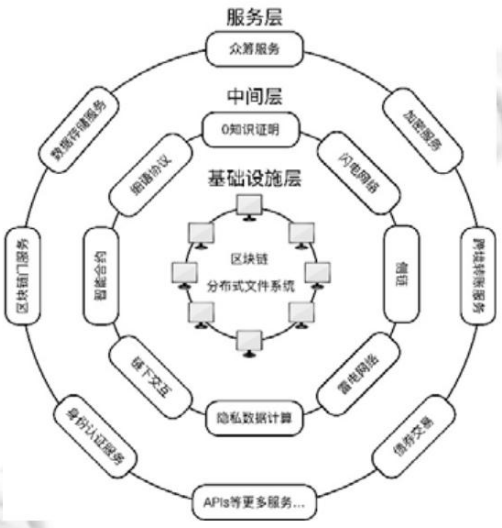

Fig.4 The architecture of BaaS

图 4 区块链即服务架构图

2.1 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。

2.2 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.在峰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.

2.3 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.

第三章区块链即服务支撑云技术

3.1 分布式共识算法

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、VRR、MultiPaxos、FastPaxos 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”,包括 Basic Paxos、Egalitarian 、Paxos、PBFT、PoW、PoS 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。Proof of Luck 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.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。

3.2 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.

3.3 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.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。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。

3.4 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)和谷歌文件系统(GFS),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,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。IPFS 能给我们一个可信的、 扁平化的、永久存储的互联网。

3.5 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。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)。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 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。

第四章区块链即服务的典型应用

4.1 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 24x7 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。

4.2 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。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。

第 5 章 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。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。