可信区块链推进计划
TRUSTED BLOCKCHAIN INITIATIVES

# 区块链即服务平台BaaS白皮书

## （1.0版）

可信区块链推进计划

2019年1月

# 版权声明



牵头编写单位：中国信息通信研究院
华为技术有限公司
腾讯云计算（北京）有限责任公司
上海点融信息科技有限责任公司

参与编写单位：杭州趣链科技有限公司　北京奇虎科技有限公司
北京百度网讯科技有限公司　阿里云计算有限公司
联动优势科技有限公司　腾讯科技（深圳）有限公司
西安纸贵互联网科技有限公司　中兴通讯股份有限公司
智链数据科技（南通）有限公司　上海淳麒金融信息服务有限公司
中链科技有限公司

编写组成员：魏　凯　卿苏德　杨白雪　张　煜　敖　萌　肖诗源　张　帅
李连港　梁　超　范锦锋　张　戈　杨　晨　张建俊　易晓春
李　磊　董　宁　张一杰　余　珊　李　凯　曹　朝　蔡春瑜
刘再耀　邵　兵　吴　非　刘　尧　王利凯

# 序　　言

自2008年末中本聪发布比特币白皮书所标志的区块链诞生，至本白皮书初版发布，已经过去了整整十年。这十年间，区块链从鲜为人知到家喻户晓，从街谈巷议到饱受质疑，其过程不可谓不惊心动魄，跌宕起伏，像极了上世纪九十年代Tim Berners-Lee发明了万维网的最初十年。很多人喜欢将区块链网络类比于互联网，因为区块链构建的是一种价值网络。当然二者其实是很不一样的，但无可非议的是，区块链会成为未来社会的一种基础设施，大量的应用将会构建在区块链网络之上。

区块链即服务（Blockchain as a Service, BaaS）平台便是为构建区块链的基础设施所做出的重要努力。BaaS平台旨在提供创建、管理和维护企业级区块链网络及应用的服务，能够帮助用户降低开发及使用成本。通过BaaS平台提供的简单易用、成熟可扩展、安全可靠、可视化运维等设计特色，区块链开发者能够满足快速部署、高安全可靠性的需要，为企业高效地开发出区块链应用。

本白皮书由浅及深地介绍了区块链即服务平台的技术细节与应用场景。基本的模块设计从功能上可划分为资源管理层、区块链底层技术和平台管理层三个层次，其底层的关键技术包括可插拔的共识机制、高可用存储和多类型账本支持、多类型的交易模型、多语言支持的智能合约引擎以及安全隐私保护。除了这些基本的区块链特性之外，BaaS平台还会提供跨云部署、跨链交互、链上链下访问和分布式身份管理等高阶特性。最后，本白皮书还分享了几个基于BaaS平台落地的重要案例，为区块链应用的开发和创新提供多视角的思路。

该白皮书是可信区块链推进计划在区块链即服务平台领域的第一个白皮书，由于编写时间仓促，该白皮书存在一定的不足，欢迎业内各界人士沟通交流讨论。

# 目录
CONTENTS

# 1 概述

## 1.1 区块链技术的背景

2008年11月，一位自称中本聪的密码学家发表了论文《比特币：一个点对点的电子货币系统》。论文描述了一种完全去中心化的数字货币，而区块链作为其底层技术从此开始进入公众视野。经过十年发展，区块链正逐渐成为最有可能改变世界的技术之一。引用维基百科中对于区块链的描述：区块链（Blockchain或Block chain）是借由密码学串接以保护内容的自增长的交易记录列表（又称区块）。每一个区块包含了前一个区块的哈希值、本区块的时间戳记以及交易数据（通常用默克尔树结构的哈希值表示），这样的设计使得区块内容具有难以篡改的特性。用区块链能让多方有效记录交易，且可永久查验此交易。狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来操作数据的一种全新的分布式基础架构与计算方式。

比特币是加密数字货币的代表。比特币出现之后，莱特币、零币、PPCoin、Ethereum等数字货币如雨后春笋般涌现出来，这些加密货币实验或许将促进人类货币体系的进一步发展。随着以比特币为首的数字货币受到越来越多的关注，人们开始将区块链技术应用到金融领域，为区块链系统引入“智能合约”技术。智能合约是一种通过计算机语言实现的旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约技术对区块链的功能进行了拓展。自此，区块链发展进入第二阶段：可编程金融。有了智能合约系统的支持，区块链的应用范围开始从单一的货币领域扩大到涉及合约共识的其他金融领域，区块链技术得以在股票、清算、私募股权等众多金融领域崭露头角。随着区块链技术的进一步发展，其“开放透明”、“去中心化”及“不可篡改”的特性在其他领域逐步受到重视。各行业专业人士开始意识到，区块链的应用也许不仅局限在金融领域，还可以扩展到任何需要协同共识的领域中去。于是，在金融领域之外，区块链技术又陆续被应用到了公证、仲裁、审计、域名、物流、医疗、邮件、鉴证、投票等其他领域，应用范围逐渐扩大到整个经济社会。除此以外，人们还试图将区块链技术应用到物联网中，实现人与人、人与机器

的万物互联。整个社会将逐渐进入智能互联网时代，最终形成一个可编程的社会。

## 1.2 企业级区块链服务的意义

区块链的行业应用正在加速推进，由数字货币等金融应用向非金融领域进行渗透扩散。企业应用是区块链的主战场，具有安全准入控制机制的联盟链和私有链将成为主趋势。云的开放性和云资源的易获得性，决定了公有云平台是当前区块链创新的最佳载体，区块链与云计算的结合越发紧密，有望成为公共信用的基础设施。在区块链应用安全方面，区块链安全问题日益凸显，安全防卫需要从技术和管理全局考虑，安全可信是区块链的核心要求，标准规范性日趋显得重要。此外区块链技术与监管要求存在一定差距，但距离有望进一步缩小。

什么领域适合区块链技术？我们认为在现阶段区块链适合的场景有三个特征：第一，存在去中心化、多方参与和写入数据的需求；第二，对数据真实性要求高的场景；第三，初始情况下相互不信任的多个参与者建立分布式信任的需求。如图1所示在传统的多个企业业务系统中，会存在信息孤岛、互相没有建立可信机制、多方协作困难效率低等难题，在该情况下可以考虑采用区块链系统。


图1 传统企业业务系统中的现有问题

典型的应用案例如：基于区块链进行货物跟踪的应用，该应用提升了数据安全性、隐私性、共享性，解决了商品转移过程中的追溯防伪问题，有效提高物流行业在结算处理效率，节约20%以上物流成本；基于区块链打造的供应链金融平台，加强了供应链金融业务中多方信息的共享，简化企业间的互担保、风险分摊、机构信用评估等流程，提升企业融资效率，融资过程从半个月降低到2天，同时也降低违约处理成本；基于区块链实现数据内容版权确权平台，数据内容版权公司能够为海量作品提供低成本、高效率的版权存证方案，版权存证时间由10–20天提升到实时版权存证，促进版权合理合法的快速流通。

可以预见，区块链是企业合作的基础信息技术，逐渐成为未来互联网企业应用不可或缺的一部分。同时区块链技术未来也将逐步适应监管政策要求，成为监管科技的重要工具。

## 1.3 常见的企业级区块链系统

### 1.3.1 Hyperledger Fabric

Linux基金会2015年成立了超级账本（Hyperledger）项目来推动跨行业区块链技术。该项目并未严格定义区块链标准，它鼓励通过社区来合作推动区块链技术，鼓励开源知识产权，采用随时间不断发展的关键标准。同时，Hyperledger是一个为了提高跨行业的区块链技术的开源全球合作项目，囊括了金融、银行、物联网、供应链、制造和科技产业的领导者。其下属的主要框架项目除Fabric以外还有Sawtooth、Iroha、Burrow、Indy等项目。

Hyperledger Fabric最早是Digital Asset和IBM组织的编程马拉松的产物，并被贡献给Linux基金会。像其他区块链技术一样，它有一个账本，使用智能合约，是一个由参与者共同管理交易的系统。Hyperledger Fabric和公有区块链系统不同之处在于它是私有的和有准入资格授权的。Hyperledger Fabric的成员要在会员服务提供商（MSP）注册。Hyperledger Fabric也提供一些可插拔的选项。账本数据能够以多种格式存储，一致性机制可以引入也可以退出，并且支持不同的多个MSP。Hyperledger Fabric还提供创建通道（Channel）的能力,允许一组参与者建立一个单独的交易账本。Hyperledger Fabric的账本系统包含两个组件：世界状态和交易日志。每个参与者都可以有一份他们参与的Hyperledger Fabric区块链网络的账本副本。世界状态组件描述了一个当前时间点的账本状态，它是账本的数据库；交易日志组件记录所有导致世界状态改变的交易，它是世界状态的更新历史记录。这样，账本就是世界状态数据库和交易日志历史的组合体，账本有可修

改的世界状态数据库。

Hyperledger Fabric中的节点具有不同角色，分别是排序节点（Orderer）、背书节点（Endorser Peer）和记账节点（Committer Peer）。Hyperledger Fabric中的交易信息统一由排序服务节点处理，保证每个节点上的交易顺序一致，天然避免了分叉问题。每个参与区块链网络的组织，可以控制多个节点，以解决组织间权利不对等的问题。

在Fabric还引入了通道（Channel）的概念。一般情况下，一个区块链网络的子链是按照“1个通道+N个成员”的基本组成。通道是区块链成员中两个或多个成员之间通信的私有“子网”，用于进行需要对其他成员做数据保密的交易。在Fabric中，建立一个通道相当于建立了一个子链。创建通道是为了限制信息传播的范围，是和某一个账本关联的。每个交易都是和唯一的通道关联的，可以明确地限定哪些成员能够知道这个交易。

在 Fabric 中，智能合约程序也叫链码（Chaincode），可以用Node.js、Java和Go等语言进行开发。Fabric上的链码分为系统链码和用户链码。系统链码用于实现系统层级的功能，包括系统的配置，用户链码的部署、升级，用户交易的签名和验证策略等。用户链码用于实现用户的应用功能，即具体的业务逻辑。开发者将链码部署到Fabric网络上，终端用户通过与网络节点交互的客户端应用程序调用链码。链码被编译成一个独立的应用程序，运行于相互隔离的 Docker容器中，在链码部署的时候会自动生成合约的Docker镜像。

### 1.3.2 Ethereum

Ethereum（以太坊）是一个基于区块链技术的去中心化应用平台，它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用。

以太坊普遍被认为是区块链2.0时代的代表性产品，创始人Vitalik Buterin于2013年底发布了以太坊白皮书，标志着该项目正式启动。2015年7月，发布了Frontier阶段，以太坊主网正式上线。2016年以太坊发布了第二个重大版本Homestead。 2017年10月，以太坊发布了第三个版本的Byzantium部分。至此，以太坊已经发展成为了区块链世界最重要的一个平台，大量的DApp（分布式应用）基于以太坊来开发。

就像比特币一样，以太坊是去中心化的，由全网共同记账，账本公开透明且不可篡改。没有任何人或者组织能够控制以太坊区块链，任何新添加的数据都需要获得全网的一致认可。

与比特币不同的是，以太坊是可编程的区块链，它提供了一套图灵完备的脚本语言。

以太坊平台对底层区块链技术进行了封装，让区块链应用开发者直接基于以太坊平台进行开发，只须专注于应用本身而无须实现区块链底层代码。以太坊上的程序被称为智能合约，它是代码和数据（状态）的集合。开发人员可以直接用以太坊原生支持的Solidity语言编写和区块链交互的智能合约，大大降低了区块链应用的开发难度。

EVM（以太坊虚拟机）：EVM是以太坊的核心，它能执行遵守协议的任何复杂的代码。EVM是图灵完备的，开发者可以在虚拟机上使用Solidity编程语言来创建应用。智能合约与链上数据的交互，也由EVM负责中间的交互过程。EVM是以太坊智能合约的运行时环境．它不仅仅是个沙盒，而是完全隔离的。这意味着代码在EVM中运行时没有办法连接网络，文件系统或者其他进程，甚至一个智能合约没有办法访问另一个智能合约。为了解决支持图灵完备下的可终止性问题以及避免网络滥用，以太坊引入了Gas概念。EVM中的每步操作和每个账本存储都会对应于一定的Gas消耗；当Gas消耗完后合约即会被终止。Gas方式相当于即时付费的手续费模式，目前被大多数的公有区块链平台所采用。

账号是以太坊的基本单元，每一个账号都有一个20个字节长度的地址。以太坊区块链跟踪每一个账号的状态，区块链上所有状态的转移都是账户之间的以太币和信息的转移。以太坊有2种账户类型，外部账号简称EOA，是由私钥来控制的。合约帐户，由合约代码来控制，且只能由一个EOA账号来操作。

交易在以太坊中是指签名的数据包，这个数据包中存储了从外部账户发送的消息，交易包含以下内容:

- 消息的接收者；
- 一个可以识别发送者的签名；
- 发送方给接收方的以太币的数量；
- 一个可选的数据字段；
- 一个 GasLimit 值，表示执行这个交易允许消耗的最大计算步骤；
- 一个 GasPrice 值，表示发送方的每个计算步骤的费用。

目前以太坊采用了ethash共识算法，本质上这是PoW共识算法。依靠大量的哈希计算来找出一个符合规定难度的当前区块的哈希值，以此来证明记账节点的工作量。其优点是安全可靠，缺点是耗费了大量的能源。

### 1.3.3 Quarum

Quorum是J.P.Morgan集团开发的一条基于以太坊的联盟链，用来向用户提供企业级分布式帐本和智能合约开发，适用于高速交易和高吞吐量处理联盟链间私有交易的应用场景。其主要设计目的是解决区块链技术在金融及其它行业应用的特殊挑战。

Quorum的设计思想是尽量使用以太坊现有的技术，而不是重新研发一条全新的链。通过合理的设计，尽量减少与Ethereum的耦合从而保持与以太坊公链的版本一致性。其主要的逻辑功能都位于专门设计的抽象层中。相比以太坊，Quorum使用了RAFT共识算法、增加了隐私性设置、对网络和节点进行了权限管理。

隐私性是Quorum的重要部分，Quorum将交易和数据进行了隐私性隔离，包括加密和零知识证明等。创建交易时，允许交易数据被加密哈希替代，以维护必需的隐私数据。在将隐私性相关功能抽象出来以后，导致的一个结果就是，状态数据库的分裂。

在以太坊中，MPT（Merkle Patricia Trie）主宰的状态树控制着整个以太坊的世界。但是在Quorum中，公有的数据仍然保持在全局状态的更新，但是私有的数据不被更新到全局状态中，而是被加密保存到节点上，同样通过分布式的事务等同步到所有的节点上。

### 1.3.4 Corda

Corda是由R3CEV推出的一款分布式账本平台，其借鉴了区块链的部分特性，例如UTXO模型以及智能合约，但它在本质上又不同于区块链，并非所有业务都适合使用这种平台，其面向的是银行间或银行与其商业用户之间的互操作场景。Corda 是一个开源的分布式账本平台，用来记录、管理和同步协议和交换价值。它从最初就是为了商业世界而设计的。Corda 允许构建可以直接交易的共同协作的分布式账本网络，而且具有严格的隐私性。

在Corda的网络中没有全局广播的操作。每个Corda网络都会有一个network map service，它发布了能够联系到网络中每一个节点的地址，还有这些节点的身份证书，还有这些节点所能提供的服务。

Corda合约就是一段验证逻辑代码，这个代码是被JVM编程语言所编写的，比如Java或者Kotlin。合约的执行需要有一个确定性结果，并且它对于一个交易的接受是仅仅基于交易的内容。一个有效的交易必须要被它的所有输入和输出状态中的合约接受。一个交易仅仅当被所有要求的签名方提供了签名之后才会被认为是有效的。但是，除了获得到所有人的签名，还必须要满足合约有效性才会被最终认为有效。

# 2 区块链服务BaaS的定义和设计原则

BaaS是一种帮助用户创建、管理和维护企业级区块链网络及应用的服务平台。它具有降低开发及使用成本，兼顾快速部署、方便易用、高安全可靠等特性，是为区块链应用开发者提供区块链服务能力的平台。BaaS通过把计算资源、通讯资源、存储资源，以及上层的区块链记账能力、区块链应用开发能力、区块链配套设施能力转化为可编程接口，让应用开发过程和应用部署过程简单而高效，同时通过标准化的能力建设，保障区块链应用的安全可靠，对区块链业务的运营提供支撑，解决弹性、安全性、性能等运营难题，让开发者专注开发。


图2 区块链即服务平台在云体系中的位置

BaaS是加速区块链在各行业落地，特别是与实体经济深度融合的重要服务形态。目前BaaS最流行的模式是区块链云服务，狭义上也把BaaS称作区块链云服务。如图2所示， IaaS是把计算资源作为服务，PaaS是把软件研发的平台作为服务，SaaS是把软件作为一种服务。BaaS作为一种云服务，是区块链设施的云端租用平台，其多租户特性让计算资源、平台资源、软件资源得到了最大程度的共享。BaaS提供节点租用、链租用以及工具租用的能力，其中工具包括开发工具、部署工具、监控工具等，并通过大容量的资源

池，保障租户的业务规模可灵活弹性伸缩，租用设施可共享和独享，安全可靠运行，此外还提供必要的技术支持服务。BaaS的具体能力包括区块链节点及整链搭建的能力、区块链应用开发的能力、区块应用部署的能力、区块链运行监控的能力。

区块链服务致力于提供企业级区块链基础技术平台，基于面向服务的基础设计原则，设计上应当以简单易用、成熟可扩展、安全可靠、可视化运维等为主要方向，携手合作伙伴为用户快速、低成本地搭建安全、高效、可靠、灵活的企业级区块链解决方案和应用。

简单易用：在开源组件基础上部署企业级分布式区块链系统并非易事，不仅需要专业的区块链知识，同时需要各种复杂的设计和配置，且极易出错。区块链服务需要帮助企业实现自动化配置、部署区块链应用，并提供区块链全生命周期管理，让客户能够容易地使用区块链系统，专注于上层应用的创新和开发。

灵活扩展：区块链服务设计应采用抽象架构和可插拔模块，面向接口设计软件，将网络构建、加密、共识、资源管理、用户管理、运维管理等功能模块分开设计实现，并可将网络构建、共识等区块链底层技术打包，作为一个插件来进行实现。系统应提供计算资源、存储资源、网络资源的无缝扩展。区块链服务也可遵循秉承源于开源、优于开源、回馈开源的原则，积极投入和引领开源社区，为用户提供成熟先进的区块链系统。

安全可靠：区块链服务应具有有效的防篡改机制、清晰的崩溃容错安全边界、安全的数据管理和隔离机制，支持核心技术如共识算法、同态加密、零知识证明、电信级云安全，高速网络连接、海量存储等，提供完善的用户、秘钥、权限管理、隔离处理、可靠的网络安全基础能力、分类分级故障恢复能力和运营安全。

可视运维：区块链服务应提供故障分类分级报警体系和运维方法，提供必要的运维接口和运维授权的能力，为链代码和链上应用提供全天候的可视化资源监控能力，为基于权限的分权分域提供完善的用户管理体系。

云链结合：区块链具备多方参与、多中心、可追溯、防篡改的特点，只有与具体的企业应用、行业场景相结合才能真正产生价值。结合云平台提供各种区块链需要的无限可扩展的资源和丰富多样的云计算产品、定制化的各行业解决方案，云链结合可以给企业带来更大的便利、价值和想象空间。

合作开放：区块链服务专注于底层技术和平台服务能力搭建，和各行业合作伙伴携手合作，共同打造可信的行业区块链解决方案和区块链生态，共同推进区块链场景落地，帮助客户实现商业成功。

# 3 区块链服务BaaS的总体架构

在BaaS设计原则的指导下，为解决区块链在企业级场景下的一些突出问题，包括系统性能、功能完备性、系统扩展性、易用性等，区块链服务可采用分层架构设计、云链结合、优化共识算法、容器、微服务架构、可伸缩的分布式云存储技术等创新技术方案，通过分层架构设计为企业提供全方位的区块链服务，帮助企业快速简单地落地区块链场景。

区块链服务BaaS的架构如图3所示,包括管理平台和运行态两个部分。管理平台分为：底层资源的管理，比如云资源管理、云资源适配器管理等；针对区块链组件的管理配置，比如区块链的部署配置、智能合约管理、动态联盟管理、区块浏览器以及链码和链上应用的监控等；平台管理主要是对使用区块链系统的用户提供更为广义和通用的管理服务如账户管理、日志管理、安全防护、计费管理、系统资源监控等。

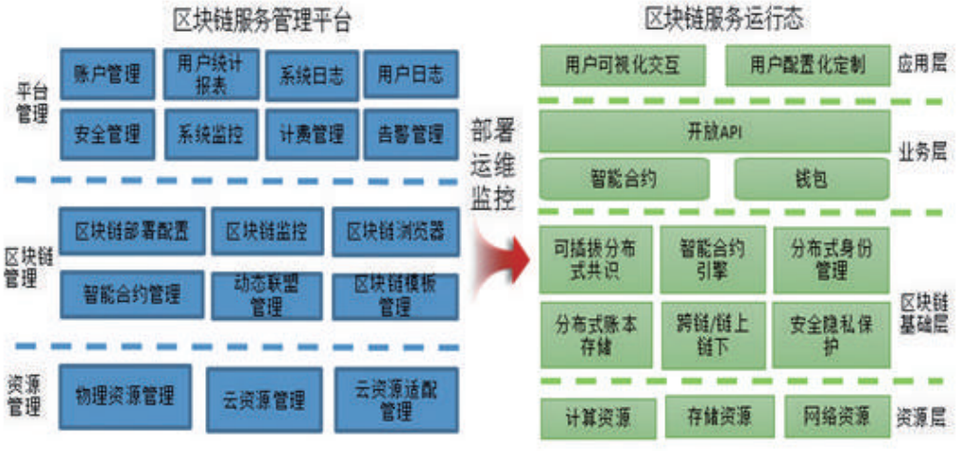


图3 区块链即服务平台BaaS的总体架构

区块链服务的运行态包括四个层面：自底向上为底层资源层、区块链基础层、业务层和应用层。

资源层包括计算资源、通讯资源、存储资源等IaaS服务，为区块链系统提供无限扩展的存储、高速的网络、按需购买弹性伸缩和故障自动恢复的节点等区块链资源。

区块链基础层可在开源的（如Hyperleger Fabric，Corda，EEA等）或闭源的（如TrustSql，蚂蚁区块链等）区块链框架上构建，为上层应用低成本、快速地提供高安全、

高可靠、高性能的企业级区块链系统。该层需要解决提供的核心技术包括可插拔的分布式共识机制、多类型的分布式账本存储机制、安全多语言支持的智能合约引擎、跨链和链上链下的数据交互、安全隐私保护以及分布式身份管理等。

业务层提供标准智能合约接口和用于个人资产管理如通证（token）的轻钱包，用户可以根据不同应用场景构建不同的智能合约，为用户打造特定场景通用的智能合约库如供应链管理和溯源、供应链金融、数字资产、公益慈善和互联网保险等，企业可以在此基础上快速构建区块链应用。

应用层为最终用户提供可信、安全、快捷的区块链应用，用户可以使用其提供的各种解决方案（供应链金融解决方案、电商行业解决方案、游戏行业解决方案、零售行业解决方案、新能源行业解决方案等等），结合合约层快速搭建区块链应用。

# 4 区块链服务BaaS的基本模块设计

区块链服务BaaS的设计主要分为管理平台设计和底层关键技术设计两大部分，每个部分的设计细节如下。

## 4.1 区块链服务管理平台的设计

根据区块链服务管理平台常见模块的功能，可以将模块分为三个层次：资源管理层、区块链管理层和平台管理层。

资源管理层中的模块负责和基础设施服务（IaaS）层的云平台交互，管理虚拟机（Docker容器）和网络等相关资源。一些并不基于云平台搭建的区块链服务BaaS平台可以直接管理底层的物理机资源。

区块链管理层的模块负责平台区块链的创建、管理和运维监控，面向的是平台用户。该层的实现由于支持的底层区块链不同，在实现上可能有较大的差异。而且有的区块链管理层可以支持多种不同的底层区块链。

平台管理层的模块负责区块链服务平台自身的账户、计费、日志和统计报表等管理功能，面向的是平台管理员和用户。

区块链服务平台主要模块和层次划分请参考图4。

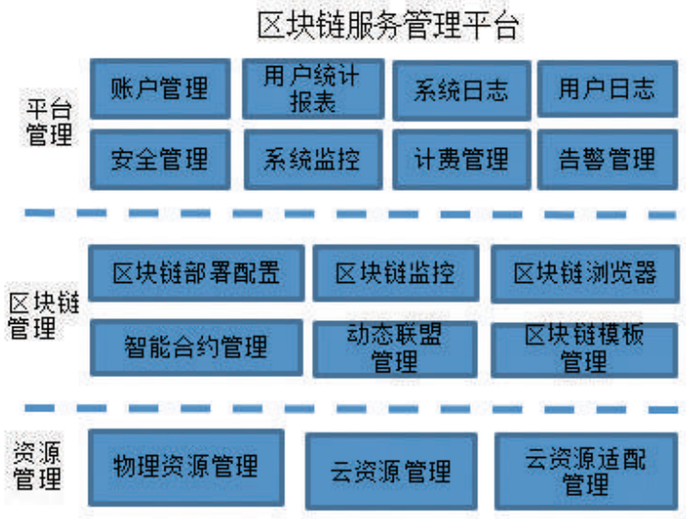


图4 区块链服务管理平台模块设计

#### 4.1.1 云资源适配管理

对区块链节点的跨云部署支持，需要由该模块来实现对不同公有云、私有云的虚拟机、Docker容器等资源调度API的封装，屏蔽各种云平台API的差异性，对上层调用模块提供统一的资源管理接口。

#### 4.1.2 云资源管理

负责实现云资源的管理调度，该模块会调用云资源管理适配模块的统一接口，所以底层不同云平台接口的差异性对该模块是透明的。该模块的主要功能有创建及删除虚拟机（Docker容器）和网络资源、进行初始化配置、对已有资源进行扩容或缩容等操作。

#### 4.1.3 区块链部署配置管理

该模块既负责对新建区块链节点进行快速安装、配置、部署以及初始化等操作，也负责对已有区块链节点进行软件升级等操作。该模块需要有较好的多节点并行处理能力，以便在部署大规模区块链网络时，可以有效地缩短安装部署时间。

考虑到用户业务需求的多样性，区块链服务平台需要支持用户可以定制符合业务场景的区块链和计算资源。例如，配置适当的区块链运行参数（出块时间，区块大小，交易数量等），选择适当的共识算法，设置各类节点的数量以及各个节点的CPU、内存、存储、网络带宽等计算资源。

对于支持动态配置的区块链，用户可以随时调整运行中的区块链的配置信息。对于基于云的区块链服务平台，用户还可以根据业务的变化情况，快速调整计算资源，比如扩大存储容量、加大网络带宽等。

#### 4.1.4 智能合约管理

用户在区块链服务平台对智能合约的管理主要有上传、发布、审核、安装、初始化、权限设置、升级等功能。

根据区块链服务平台的能力，用户可以上传源代码形式的智能合约，也可以上传编译好的二进制智能合约到平台上。

用户上传的智能合约被存放在平台上的用户个人智能合约库中，需要用户将智能合约发布到区块链上，才可以被该区块链上的其他成员审核和使用。用户发布智能合约时，也可以设置哪些该区块链中的参与方可见，对智能合约的使用权限做相应的控制。

在线审核功能一般针对以源代码形式上传的智能合约，区块链上的各个成员可以对智

能合约的源代码进行检查，确保各项功能正确无误。

对具有智能合约商店的区块链服务平台，用户可以从智能合约商店购买智能合约。用户购买的智能合约也被存放在平台上的用户个人智能合约库中。以后的使用也遵循发布、审核、安装、初始化的流程。

在合约初始化的过程中，用户不仅可以初始化合约内容，对合约的背书策略、安全策略也可以进行相应的设置。合约升级过程中，要保证原合约可以使用。升级过后，新合约可以查询到历史数据。对于合约的权限，平台提供多维度的权限管理，例如方法级权限、数据级权限等。用户可以通过BaaS平台提供的接口或者网页，查询合约的运行日志，分析合约的运行状态等。

智能合约的升级也是相同的管理流程，只是此时用户使用的是更新版本的智能合约。

#### 4.1.5 动态联盟管理

联盟链一般都有多个成员参与，动态联盟管理是联盟链顺利运作的基础。联盟管理包括，联盟链的创建，联盟链新成员的加入、联盟链已有成员的退出、联盟链的投票策略设置等功能。不少区块链服务平台的联盟链中，有管理员的角色，一般由联盟链的创建者担任。管理员主要负责联盟链的创建，初始配置的设置，联盟链成员管理和权限管理等等。很多区块链服务平台为了防止管理员的权力过大，往往引入成员投票机制，比如只有在联盟链已有成员多数同意的情况下，才允许新成员加入该联盟链。

#### 4.1.6 区块链模板管理

因为区块链配置的高度复杂性，如果全部开放给用户设置，会带来较大的使用难度。为了方便用户的使用，平台管理员可以针对一些典型的区块链应用场景，预先制定相应的区块链模板，配置好缺省的参数。用户创建区块链时，只需根据自己的业务场景选择相应的预定义模板，就可以快速方便地创建满足需求的区块链。高度可定制的区块链配置和预定义区块链模板的结合，可以让区块链服务平台同时兼顾区块链可定制性和易用性。

#### 4.1.7 区块链监控

区块链监控模板负责对区块链网络和节点的运行状况进行监控报警,包括但不限于网络连通性监控、计算资源使用情况监控以及节点服务状态监控。一旦发现有故障或者异常情况发生，可以自动给相关负责人通过邮件、短信等方式报警。在某些情况下，平台可以自动进行故障排除和恢复。

#### 4.1.8 区块链浏览器

区块链浏览器可以让用户查询区块链高度、交易数量、网络拓扑、安装的智能合约列表、具体交易情况等区块链细节信息，帮助用户更好地了解区块链运行状态以及进行相关开发调试。区块链服务平台对区块链浏览器有相应的权限控制，以免用户信息泄露。

#### 4.1.9 账户管理

账户管理是区块链服务平台的重要功能，一般分为管理员账户和用户账户。管理员账户是平台运营方用于平台本身设置管理的，具有最高的权限。用户账户由平台的客户创建，可以根据业务需要在平台上创建一个或多个区块链。

#### 4.1.10 用户日志

平台需要通过用户日志来记录用户在平台执行的各项操作，比如创建和删除区块链、增加和删除节点、安装智能合约等。用户可以通过用户日志来查询自己做过的历史操作记录，方便用户管理区块链。

#### 4.1.11 系统监控

与区块链监控模板不同，系统监控模块用于监控区块链服务平台自身的运行状况，比如用户操作的响应时间、区块链创建时间、在线用户数等指标。通常只有平台管理员有权查看系统监控数据。

#### 4.1.12 计费管理

区块链服务平台可以根据平台的定价策略，对用户使用平台的计算资源和服务计算相关费用。通常可以分为按服务使用时间和使用次数计费两种方式。

### 4.2 区块链底层关键技术

区块链的技术架构设计可以分为核心技术组件、核心应用组件以及配套设施，它们相互独立但又不可分割，具体架构图如图5所示。核心技术组件在逻辑上也称协议层，包括区块链系统所依赖的基础组件、协议和算法，进一步可以细分为共识机制、安全机制、账本存储、节点通信共四层结构。

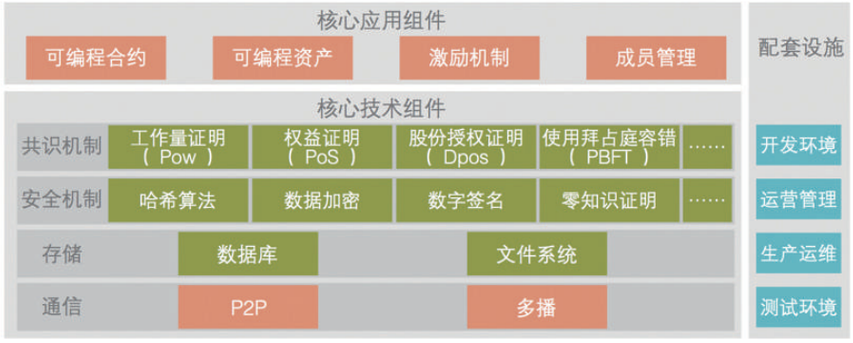


图5　区块链的底层技术架构

### 4.2.1　可插拔的共识机制

所谓共识，是指多方参与的节点在预设规则下，通过多个节点交互对某些数据、行为或流程达成一致的过程。共识机制是指定义共识过程的算法、协议和规则。区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果，直接被其他节点认同后并最后有可能成为最终共识结果。区块链系统中需要支持可插拔的共识机制， 允许用户在不同的应用场景中选择适合的共识算法，目前业界常用的共识算法包括PoW（Proof of Work）工作量证明机制、PoS（Proof of Stake）股权证明机制、DPoS（Delegated Proof-of-Stake）委托权益证明机制、PBFT（Practical Byzantine Fault Tolerance）实用拜占庭容错机制等。

工作量证明机制通过计算来猜测一个随机数值，以解决规定的哈希计算问题来获得记账权。在比特币中，所有的节点都是平等的，即人人都有记账的权利，记账就是将节点交易池的一定量交易按时间顺序打包成区块。当每个人都拥有记账权时都可以进行打包，而各节点的交易池由于网络延迟等各种问题存在一定的差异，整个网络中就会存在各种大同小异的账本，如何在保证节点记账权利的基础上做到全网共用一个账本就成了共识算法的关键设计点。中本聪想到的是给记账加入工作成本，即区块链由各个区块按照时间先后排序，每个区块设立难度值，节点通过不断变化一个随机数进行哈希计算以期完成难度值设定。这给记账增加了难度，同时通过对难度值的调整，可以调节在一定时限内只有少部分人可以完成工作量的证明。此外PoW算法还需遵循两个原则：一个是最长链原则，即视最长的链为正确的区块链；另一个是记账激励原则，即成功挖出合法区块的账户可以得到网络的奖励。

股权证明机制是在2011年由一个名为Quantum Mechanic的数字货币爱好者在Bitcoin Talk论坛中提出的。经过充分讨论,尤其是以以太坊（Ethereum）为首的致力于公链建设的组织机构的不懈研究，证明其具有可行性。不同于PoW中记账权的获取主要通过算力进行竞争，即节点提供的算力越大，成功挖出区块获得收益的概率也就越大，PoS记账权的获取依赖于节点的资产权重,即账户资产越大，越容易获取记账权完成出块。与此同时，PoS还运用经济学中的博弈论原理来限制恶意节点的作恶行为，即如果恶意节点作恶被发现，将被没收部分甚至全部资产，造成直接的经济损失。另外，PoS也借鉴了拜占庭容错算法，对于节点中还是可能存在的分叉，可以进行PoS投票，全网超过2/3的资产所有者认同的链就是正确的区块链。

委托权益证明机制基于PoS算法，能够让每一个人选出可以代表自己利益的人参与到记账权的争夺中，这样多个小股东就能够通过投票选出自己的代理人，保障自己的利益。DPoS算法在任何可想到的自然网络中都是安全，甚至面对足够多的少数群体的勾结。与一些类似算法不同的是，DPoS在大多数生产者失败的情况仍可继续工作。在这种情形下，社区可以投票来替换失效的生产者，直到恢复到100%的参与度。目前没有其它的共识算法可以在这样的高失败或变动的网络情况下保持足够的健壮，最终DPoS从选择区块生产者算法选择获取了显著的安全性。

拜占庭问题又称为拜占庭将军问题（Byzantine Generals Problem），是Leslie Lamport于1982年提出用来解释一致性问题的一个虚构模型。对于可靠的计算机系统来说，故障部分必须可以通过系统的不同部分提供的冲突信息进行正确的判断，这种情况可以用拜占庭军队中的一群将军围绕敌城驻扎进行抽象的表达：将军们只能通过信使沟通，必须就共同的战斗计划达成一致。但是，他们中的一个或多个可能是叛徒，他们会试图混淆其他人。问题就是找到一个算法，以确保忠诚的将军达成一致。结果表明，只有口头信息，当且仅当三分之二以上的将军忠诚时，这个问题是可以解决的。对于拜占庭问题来说，假如将军总数为N，叛变的将军数为f，则当N>=3f+1时，问题才有解，该问题的解即拜占庭容错算法（Byzantine Fault Tolerant，BFT）。实用拜占庭容错算法（Practical Byzantine Fault Tolerance，PBFT）是Miguel Castro和Barbara Liskov在1999年提出来的，它在原始拜占庭容错算法的基础上，解决了其理论可行而实际效率低下的问题，真正实现了分布式异步共识系统中的拜占庭攻击问题，大力推动了拜占庭容错算法在实际系统中的应用。PBFT算法有三大协议，分别为三阶段共识协议，保证了主节点打包的区块通过三阶段共识完成打包结果的一致性确认，并保证应对拜占庭攻击的系统活性；视图变更协议，保证了在主节点作恶情况下，系统可以通过该协议选举出新任的主节点进行共

识，且不破坏其原有的共识状态；检查点机制，保证了各节点经过确认的一致性状态得以持久化，并且内存中的垃圾容量保持在一定限制内。

### 4.2.2 高可用存储和多类型账本支持

区块链服务BaaS通过非对称加密的数字签名保证业务请求在传输过程中不能被篡改，通过共识机制保证各节点的数据一致地存储。对于已经存储的数据记录通过节点内的自校验性和准实时多节点数据校验来保证已经存储的数据记录不能被修改。区块链中的分布式存储是指参与的节点各自都有独立的、完整的数据存储。区块链数据在运行期以块链式数据结构存储在内存中，最终会持久化存储到数据库中。对于较大的文件，也可存储在链外的文件系统里，同时将摘要(数字指纹)保存到链上用以自证。跟传统的分布式存储有所不同，区块链的分布式存储的高可用性主要体现在两个方面：首先，区块链每个节点都按照特定的存储模式存储完整的数据，而传统分布式存储一般是将数据按照一定的规则分成多份进行存储；其次，区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。数据节点可以是不同的物理机器，也可以是云端不同的实例。

“区块链”这个名字正是由于区块链底层的块链式存储而来的，但是随着区块链3.0时代的到来，越来越多的新型区块链项目提出了非块链式的存储模型。

对于块链式存储，区块链上的账本数据可以分成两部分，即区块链数据和状态数据。由于不同区块链平台选择了不同的交易记录模型，因此两类数据的记录也不尽相同，但它们对于区块链数据（包括区块和交易两部分，有些区块链平台还会包含交易回执）的存储都采取了块链式的存储模型，区块链数据主要通过区块的形式进行串联。所有区块被从后向前有序地连接在一个链条里，每一个区块都指向其父区块。区块中包含了一批交易，由共识模块负责统一打包并定序。区块链节点在接收到一个区块之后，在原有的状态集基础上，依次执行交易，在此期间读/写相关状态集。一笔交易执行结束，也就意味着区块链状态进行了一次变迁。最简单块链式存储结构如图6所示。

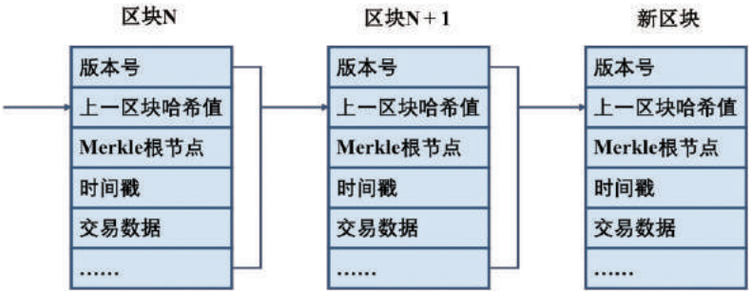


图6 区块链的块链式存储结构

对于非块式存储，典型的技术——如有向无环图(Directed Acyclic Graph，简称DAG)，可以应对安全、高并发、可扩展性和数据增长等问题，可以较好地适应小额支付场景。基于DAG的设计因为没有区块的概念，是一种新型的区块链底层存储模型，其扩容完全不受区块大小的限制，所以其可伸缩性只取决于网络带宽，CPU处理速度和存储容量的限制。Swirlds Hashgraph是一种全新的分布式账本共识机制技术和数据结构，其本质是有向无环图（DAG），并非是链式结构。Hashgraph能为分布式应用提供高效、公平、安全的基础设施。高吞吐量和异步拜占庭容错（ABFT）的特点，使得Hashgraph在公链和私有链领域都有潜在的使用价值。Hashgraph引入了Gossip协议，通过Gossip协议传播散列图，另外基于散列图做虚拟投票，有效地避免了共识过程中突发的大规模消息传递，保证了本地计算的高效性。

### 4.2.3 多类型的交易模型

在区块链网络中，目前主要存在两种交易记录模型，一个是以比特币为代表的UTXO（UnspentTransaction Output，未使用交易输出）模型，另一个是以以太坊为代表的账户/余额模型。

比特币作为最早出现的加密货币，采用了UTXO模型作为其底层存储的数据结构，也是比特币交易的基本单位。UTXO是不能再分割、被所有者锁住或记录于区块链中的被整个网络识别成货币单位的一定量的比特币货币。在比特币的世界里既没有账户，也没有余额，只有分散到区块链的UTXO。“一个用户的比特币余额”这个概念是一个通过比特币钱包应用创建的派生之物，比特币钱包通过扫描区块链并聚合所有属于该用户的UTXO来计算该用户的余额。

账户/余额模型则非常好理解，传统的账本都是基于这个模型实现的来实现的。比如有两个交易方张三和李四，我们会分别为他们创建一个账户，并记录余额。如果他们两人之间进行转账，通常的也是采用复式记账的方式，假设张三要给李四转账100元，则系统要做如下操作：

1）检查张三账户余额是否充足，如果不足100元就终止交易，向张三报“余额不足”；

2）在张三账户里减去100元（假设零手续费）；

3）在李四账户里增加100元。

这种系统很常见，现在的银行也好、信用卡也好、证券交易系统也好，互联网第三方

支付系统也好，其核心都是基于账户的设计，由关系数据库支撑。通常都是通过数据库的事务来实现操作的原子性，保证转账的双方余额的变动是同时成功或者同时失败的。

#### 4.2.4 多语言支持的智能合约引擎

一个成熟的区块链的智能合约引擎，需要提供智能合约代码上链的手段、智能合约执行的方法、链上数据的读取和操作等。通俗地说，我们可以认为智能合约上链的过程就是智能合约的初始化阶段，一般包括智能合约数据的初始化和智能合约代码存入合约账号两个方面；智能合约的执行一般是根据用户调用数据的要求执行合约修改合约数据和链上数据的过程；而链上数据的读取和操作则是合约执行的必要工具。随着智能合约在区块链技术中的广泛应用，其优点已被越来越多的研究人员与技术人员认可。总体来讲，智能合约具备合约制定的高时效性、合约维护的低成本性、合约执行的高准确性等优点。

虽然智能合约较传统合约具有明显的优点，但对智能合约的深入研究与应用仍在不断探索中，我们不能忽略这种新兴技术潜在的风险。2017年，多重签名的以太坊钱包Parity宣布了一个重大漏洞，这个关键漏洞会使多重签名的智能合约无法使用，该漏洞导致了价值超过1.5亿美元的以太坊资金被冻结。安全风险事件的发生值得我们反思。但不管怎样，业内人士普遍认为，区块链技术及智能合约将成为未来IT技术发展的一个重要方向，目前的风险是新技术成熟所必然经历的过程。

目前智能合约作为区块链的一项核心技术，已经在以太坊、Hyperledger Fabric等影响力较强的区块链项目中得到广泛应用。

1）以太坊的智能合约应用：以太坊的一个智能合约就是一段可以被以太坊虚拟机执行的代码。以太坊支持强大的图灵完备的脚本语言，允许开发者在上面开发任意应用，这些合约通常可以由高级语言（例如：Solidity、Serpent、LLL等）编写，并通过虚拟机转为位码存储在区块链上。智能合约一旦部署就无法被修改。用户通过合约完成账户的交易，实现对账户的货币及状态进行管理与操作。

2）Hyperledger Fabric的智能合约应用：在Hyperledger Fabric项目中，智能合约的概念及应用被更广泛地延伸。作为无状态的、事件驱动的、支持图灵完备的自动执行代码，智能合约在Fabric中部署在区块链网络中，直接与账本进行交互，处于十分核心的位置。和以太坊相比，Fabric智能合约和底层账本是分开的，升级智能合约时并不需要迁移账本数据到新智能合约当中，真正实现了逻辑与数据的分离。Fabric的智能合约称为链码（Chaincode），分为系统链码和用户链码。系统链码用来实现系统层面的功能，负责Fab–

ric节点自身的处理逻辑，包括系统配置、背书、校验等工作。用户链码实现用户的应用功能，提供了基于区块链分布式账本的状态处理逻辑，由应用开发者编写逻辑，对上层业务进行支持。用户链码运行在隔离的链码容器中。

总体来讲，技术人员可采用四种手段实现智能合约的多语言支持。这四套方案总结起来有两个因素，一个是已有的或新的虚拟机或平台，另一个是已有的语言或新的智能合约语言。

1) 提供新的编译器，将智能合约语言翻译到EVM或其他简易链上虚拟机或平台；

2) 改造已有成熟语言及其编译器，将其翻译到EVM或其他简易链上虚拟机或平台；

3) 改造已有的虚拟机或平台作为链上虚拟机或执行平台，同时提供把智能合约语言翻译到该链上虚拟机或平台的编译器；

4) 改造已有的虚拟机或平台作为链上虚拟机或执行平台，改造相应成熟语言的编译器来构建智能合约平台。

这四种方法各有各的好处，当前也有各大平台正在实践中。比如，以太坊当前采用的就是第一套方案，同时他们也在计划使用WebAssembly作为其链上虚拟机提供智能合约的执行平台，这个计划版本采用的就是第三套方案。NEO通过提供简易链上虚拟机，然后通过把.NET的MSIR编译到该链上虚拟机来提供所有.NET语言的支持，它采用的就是第二套方案。而EOS则是通过改造已有的WebAssembly提供其已有语言的智能合约支持，它采用的是第四套方案。

### 4.2.5 安全隐私保护

安全机制是区块链中最为核心与关键的组成部分，而密码原语与密码方案是安全机制的支撑技术。区块链系统通过多种密码学原理进行数据加密及隐私保护。区块链服务BaaS自身具备的技术和特性保证数据隐私、信息流转和网络传输的安全可控。区块链服务BaaS运用安全散列、对称加密、非对称椭圆曲线、抗量子等加密算法，以及零知识证明算法、安全多方计算等技术组合，保障数据隐私的安全，防止数据泄漏。在构建隐私保护方案的同时，需考虑可监管性和授权追踪，通过采用高效的零知识证明、承诺、证据不可区分等密码学原语与方案来实现交易身份及内容隐私保护；充分利用基于环签名、群签名等密码学方案的隐私保护机制、基于分级证书机制的隐私保护机制；也可通过采用高效的同态加密方案或安全多方计算方案来实现交易内容的隐私保护。对于公有链或其他涉及到金融应用的区块链系统而言，高强度高可靠的安全算法是基本要求，需要达到国密级别。

- 加密体系

安全散列函数（cryptographic hash function）为单向函数，即从安全散列函数的输出推算出它的输入是及其困难的，而在正向计算的时候，又应当是快速高效的。单向散列函数被称为现代密码学的根基，输入和输出分别称为消息（message）和消息摘要（message digest）。目前比较通用的安全散列函数算法有SHA家族算法、MD系列算法、RIPEMD系列算法等。在区块链应用当中，采用SHA3-256(Keccak256)算法作为安全散列算法，在目前所有安全散列算法当中最为安全，并且在业界也能够得到较为广泛的认可。

区块链系统通过多种密码学原理进行数据加密及隐私保护。在区块链中，信息的传播按照公钥、私钥这种非对称数字加密技术实现交易双方的互相信任。区块链服务BaaS采用密钥协商算法（如ECDH）、数字签名算法（如ECDSA）和非对称加密算法（如国密算法SM2）来保证数据传输的安全。

- 身份认证和权限控制

区块链技术依靠强大的密码学原理和权限控制构建了一套可信的身份验证的工具，可以建立一套身份识别系统，让企业、产品、应用和服务进行交互，有助于削减各种制度性的认证性成本和提升认证安全性保障。权限准入的概念在现有的三大类区块链体系中的表现各不相同：对于公有区块链来说，节点和客户端可以完全自由地出入区块链网络，可以自由地查看区块链上的数据，不存在权限管理的困扰；对于私有区块链来说，节点和客户端的区块链网络接入完全由个人或组织全部掌控，也不存在权限管理的困扰；只有在联盟区块链中，节点和客户端进入区块链网络需要各联盟节点的权限认证和共识。

数字证书（Digital Certificate）又称为公钥证书，是网络通信双方用于身份认证及安全通信的保障。数字证书实际上是一份电子文件，包含了拥有者的身份和公钥信息，以及证书认证机构对这份文件的签名。公开密钥基础设施（Public Key Infrastructure，PKI）采用数字证书（或者说CA证书）进行公钥管理，通过CA（Certificate Authority）机构签发包含用户信息及其公钥信息的证书，用于网络中通信双方进行身份验证和安全通信。区块链权限管理可以借鉴的方案，[XS2]区块链的节点可以简单地分为两类——共识节点（验证节点，Validate Peer，VP）和记账节点（非验证节点，Non-Validate Peer，NVP），同时还有其他的SDK权限等等，都可以通过分类CA的架设得以实现。

公有链是指全世界任何人都可读取的、任何人都能发送交易且交易能获得有效确认

的、任何人都能参与其共识过程的区块链。共识过程决定哪个区块可被添加到区块链中和明确当前状态。作为中心化或者准中心化信任的替代物，公共区块链的安全由“加密数字经济”维护。“加密数字经济”采取工作量证明机制或权益证明机制等方式，将经济奖励和加密数字验证结合了起来，并遵循着一般原则：每个人从中可获得的经济奖励，与对共识过程作出的贡献成正比。这些区块链通常被认为是“完全去中心化”的。因此在公有链当中所有的节点都是平等的。

联盟链是指其共识过程受到预选节点控制的区块链；例如，不妨想象一个有15个金融机构组成的共同体，每个机构都运行着一个节点，而且为了使每个区块生效需要获得其中10个机构的确认（2/3确认）。区块链或者允许每个人都可读取，或者只受限于参与者，或走混合型路线，例如区块的根哈希及其API（应用程序接口）对外公开，API可允许外界用来作有限次数的查询和获取区块链状态的信息。这些区块链可视为“部分去中心化”。因此在联盟链中存在认证节点以及非认证节点之分，通过证书来区别节点的身份，认证节点参与共识，而非认证节点则不参与共识。

- 隐私保护

隐私保护从被保护的主题来看可分为交易发送方的匿名隐私保护、接收方的匿名隐私保护和数据的隐私保护三大类。

交易发送方的匿名隐私保护可采用群签名或环签名等技术。群签名即在一个群签名方案中，一个群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名。与其他数字签名一样，群签名是可以公开验证的，且可以只用单个群公钥来验证。环签名由三位密码学家Rivest, shamir和Tauman在2001年首次提出，是一种简化的群签名，只有环成员没有管理者，不需要环成员间的合作。环签名方案中签名者首先选定一个临时的签名者集合,集合中包括签名者。然后签名者利用自己的私钥和签名集合中其他人的公钥就可以独立的产生签名,而无需他人的帮助。签名者集合中的成员可能并不知道自己被包含在其中。环签名与群签名类似，但在两个关键方面有所不同：一个是无法撤销单个签名的匿名性，其次是任何用户组都可以作为一个组使用，无需额外设置。

交易接收方的匿名隐私保护包括主动匿名技术和被动匿名技术。主动匿名使用的分层确定性钱包是指使用分层确定性地址机制的电子钱包，通过椭圆曲线密码学机制，确保可以通过在没有私钥参与的情况下，由公钥直接分散成子公钥，并且分散的子公钥可以由分散的子私钥认证。如比特币协议建议每次交易都尽可能使用新的地址，因为同一个地址被使用的越多，账户的相关性就越容易暴露。但是分层确认性地址机制(Hierarchical Deter–

ministic)，类似于IC卡中得密钥分散机制，能够有效解决这一问题。通过随机数机制确定一个主私钥，然后使用一个确定的、不可逆的算法，基于主私钥生成一定数量的子私钥，并将主私钥以纸钱包的方式备份、离线存放在本地端。该方案在安全、记账、备份、权限控制等方面相较于传统钱包具有明显优势。

交易接收方的被动匿名(被动隐身)中使用的隐身地址秘钥管理机制是一项用于保护加密货币接收者隐私的隐私增强技术。隐身地址要求发送方代表接收方为每笔交易创建随机的一次性地址，以便公众无法对同一收款人的不同转账进行关联。通过隐身地址机制可以有效解决管理与执法相关的问题以及隐藏接收方相关的特定敏感信息。

数据隐私保护可采用的技术如对数据的加盐加密处理、基于承诺的零知识证明、zk-SNARK及应用Z-Cash技术等。加盐加密是一种对系统登录口令的加密方式，它实现的方式是将每一个口令同一个叫做“盐（salt）”的n位随机数相关联,将口令和随机数连接起来然后一同加密，加密后的结果放在口令文件中，提高了破解难度。零知识证明(Zero—Knowledge Proof)，是由S.Goldwasser、S.Micali及C.Rackoff在20世纪80年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。使用零知识证明的本质是对链上的数据进行隐私保护，而区块链中的隐私保护问题已经成为了制约公有链发展的一个重要因素。随着人们的个人信息保护意识的提高，更加注重个人隐私的保护，或许隐私保护会成为区块链应用落地的一个大的切入点。zkSNARK（zero-knowledge Succint Non-interactive ARguments of Knowledge）具有两个特点：其一是简洁性（Succinct），即验证者只需要少量计算就可以完成验证；其二是非交互性（Noninteractive），即证明者和验证者只需要交换少量的信息即可。Zcash是zk-SNARK第一个广泛的应用，一种新型的基于零知识证明的数字货币。Zcash的强大隐私保障源自于Zcash的屏蔽交易可以在区块链上完全加密，通过使用zk-SNARK的零知识证明，让交易在全网络共识规则下仍然有效运行，且能以此途径来保证交易的发送者、接受者和交易金额的机密性。

# 5 区块链即服务平台的高阶特性

## 5.1 跨云部署

区块链服务云部署模式主要分为三类，即云上部署、云上云下混合部署以及跨云部署。针对云上部署模式，区块链所有节点部署在公有云上；针对云上云下混合部署，区块链的部分节点部署在公有云上，部分节点部署在客户私有数据中心或者私有云内；针对跨云部署，区块链的节点可以分散部署到不同的公有云平台上。

组建联盟链的各用户基于传统业务的使用习惯或者合作关系，可能对区块链节点所在的云平台具有各自的偏好。如果区块链服务能够支持跨云部署，将有利于促成这些用户更方便地组建联盟链。

区块链服务平台一般应该通过适配层来屏蔽底层公有云的差异性，为用户提供一致的云上区块链管理体验。同时因为区块链跨云部署时，节点一般走公网互联互通，所以系统设计时需要充分考虑较长的网络时延和不稳定的网络带宽带来的种种影响。

## 5.2 跨链交互

在区块链所面临的诸多问题中，链与链之间的互通性缺失很大程度限制了区块链的应用空间。跨链主要包括信息跨链和价值跨链两种应用场景。跨链互操作协议的严谨描述、规范实现和普遍应用将成为实现“价值互联网”的关键。区块链跨链互操作技术提供了同构和异构区块链之间的信息交互和价值流转服务，可以满足区块链应用的业务扩展性需求。

### 5.2.1 分层多链跨链技术

多链模型可采取如图7所示的分层结构，底层以公有链作为基础链，上层针对相互独立的子业务分别搭建不同应用联盟链的多链业务模型。应用联盟链与底层公链之间的跨链资产互换，在应用联盟链上的关键信息定时或通过事件触发跟基础公链之间进行数据交换，用以达到以公链为应用联盟链进行背书的目的，兼顾了应用联盟链的效率与底层公链的公平。

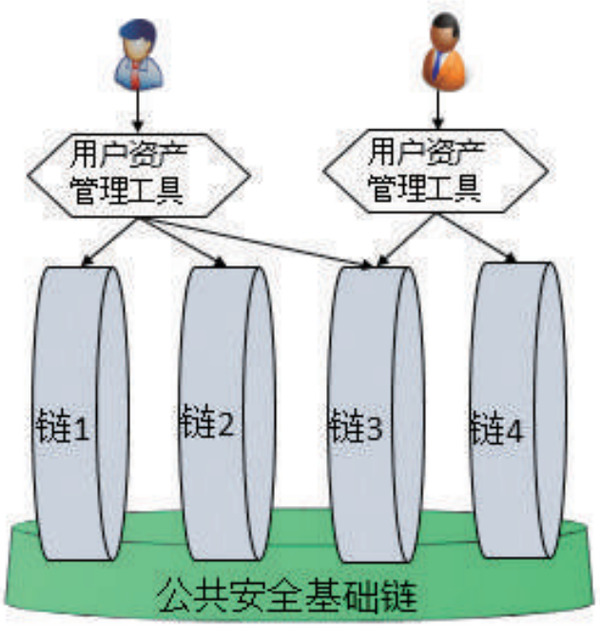


图7　基于分层结构的多链模型

多链之间交互有信息互认、跨链资产流转和服务调用等方式。跨链信息互认的案例有数字版权、公证公示、数字身份等信息的跨链访问和确认，其目的是充分利用已有资源，减少重复建设；跨链资产流转和服务调用，是通过跨链交易的定义、可信传递和验证，实现资产标识跨链转移和计算资源跨链调用，典型的场景如联盟之间的积分互换，交易所等。

### 5.2.2　一般跨链技术

跨链交互的技术模式可采用公证人模式或信息锁模式。所谓公证人模式（如图8所示），是指存在一个可信的公证人节点，此节点具有多种链打包排序、入链落块等功能和权力。跨链双方将各自的信息都提交至公证人，部分情况下需要将资产等信息都转账给公证人进行验证，公证人执行交换契约，对信息进行交换所有权、转移兑换、销毁/生成等。此模式为中心化模式，性能、安全性、可用性等完全依赖公证人节点。

所谓信息锁模式（如图9所示），是指发起人使用一个谜题和答案锁定需要交换的信息、资产，指定接收者和时间、区块高度等限制条件。限制条件之内，接收者随时可以使用答案来提取信息、资产等所有权。限制条件达成时没有被提取，则信息、资产退回给发起人。跨链参与的双方可以使用此技术完成信息跨链。

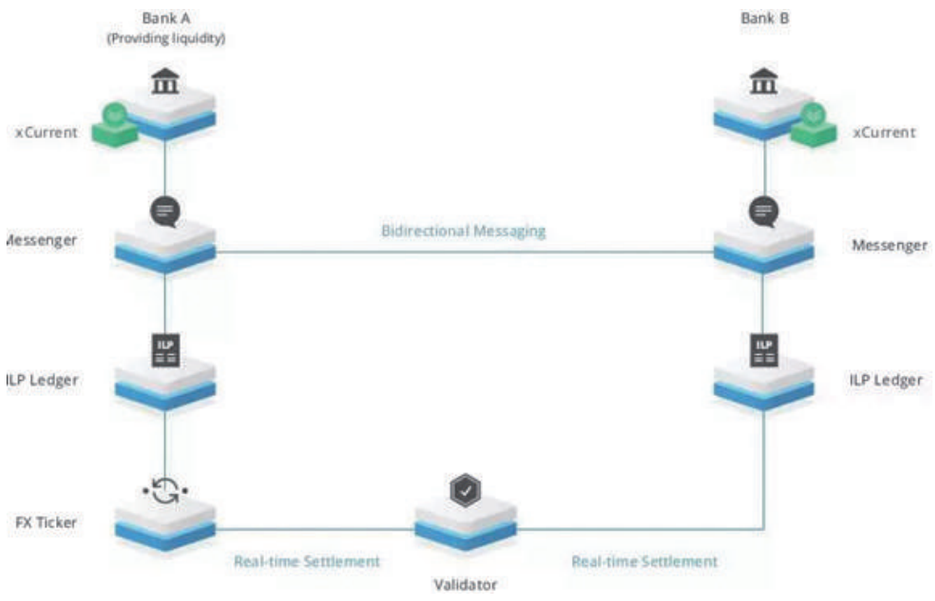


图8　基于公证人模式的跨链资产交互

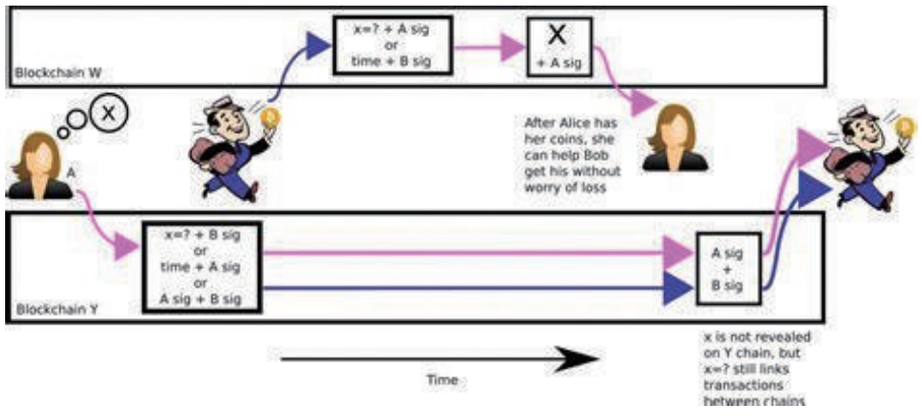


图9　基于信息锁模式的跨链资产交互

从链的设计实现结构来看，一般跨链资产交互可分为同构同链、同构异链、异构链之间的交互。

- 同构同链下的跨链交互

同构同链是指使用同一种技术创建、部署区块链。区块链节点之间的通讯协议、共识算法、数据结构、加密算法等技术皆完全相同，可称为同构。基于同一个创始区块，或类似同样的数据基点而发展来的树状、网状区块链体系，可称为同链。同链具有一个半强制性规则，即节点证书等身份信息唯一且链内共享。该模式下的跨链交互可大体分为子链回归和多子链并行的模式。

子链回归是指链结构分为主链、子链两部分。子链附属于主链，可获取主链信息。一般情况下，主链不知道子链。子链用于非冲突类并发验证，独立事件结算等，使用同一套账户证书体系，支持互验签名。由子链监听主链事件，完成信息下载；由子链发起信息上传，主链完成行为约束、信息校验、冲突校验等工作，完成跨链信息传递。必要时，子链完成信息、资产等销毁工作。子链使命完成，或信息全部回归至主链后，子链可全部销毁废弃。BaaS在此类跨链技术中扮演通道管理者角色，为各条链提供节点发现、区块查询校验、事件监听通知等功能。例如主链提供锚定资产锁定，子链完成锁定资产范围内的多次交易后回归主链，主链验证锚定有效性，并根据交易结果解锁释放资产。

多子链并行与子链回归中类似，不同的是账户证书存储在主链中，账户内事务根据离散算法，存储在固定的一条或多条子链中。当各个账户之间发生信息交互、资产交易时，触发多子链跨链通讯事件。此时由主链提供身份证明和中继通道，并约束各个子链行为。BaaS在此类跨链技术中扮演推动者角色，监听各个阶段事件，没有主动发起者的环节充当推动者，推动跨链流程完成。例如根据地理、类型等特征分组账户，将其分散在多个子链中，每个子链是一个信息域。子链内部完成内部信息交换，在主链上完成跨域信息交换。

- 同构异链下的跨链交互

同构异链为使用相同的技术，搭建多条基于各自创世区块的区块链场景。可分为账户关联和账户不关联的两种模式。

在账户关联场景下，需要同一用户在多个链上使用唯一标识注册获取证书等身份验证信息，这些身份验证信息有直接或者间接关联关系。两个账户持有者，在不同链上使用自己的身份信息进行跨链资产等信息交换。BaaS在此类跨链技术中可以负责多项职能。鉴定双方身份的公证人，信息锁传递的通道，环节推动者等。

账户不关联场景多为数据广播使用，非资产类信息在多条链上留存。BaaS在此类场景可以进行数据映射，监听A链的事件将相应信息推送至B链广播等。

- 异购链下的跨链交互

异构链是指使用不同技术搭建的区块链场景，也可分为账户关联和账户不关联两种模式。

账户关联与同构异链模式不同的是，此模式下链节点对身份信息的验证方式可能不同，在不兼容的场景下，无法直接验证对方数据有效性。需要BaaS作为中间方，提供附

加功能，如：身份管理服务器、信息锁服务器、定制化信息可信交换通道等。

账户不关联模式多为信息备份，如公有链强制分叉、公有链信息同步至私有连、联盟链信息公开至公有链等场景。BaaS 在此类场景中可以完成数据转换对接功能。

## 5.3 基于预言机的链上链下访问

作为真实世界信息进入区块链的通道，预言机为区块链提供了可信的外部数据接入服务。通过预言机服务，可以实现链下信息触发链上动作，打破区块链与现实世界的信息壁垒。预言机服务可以帮助用户的链上平台对接可靠第三方信息平台的Web API，满足其业务需求。

区块链预言机模块通过引入验证机构约束上链服务提供方，在密码学方法的辅助下，以不影响正常网络通信为前提，确保上链服务被约束为能且只能发送可信数据源提供的数据上链，且该约束过程可被验证。同时，上链服务运行在 SGX（Software Guard Extension）创建的可信执行环境（Trusted Execution Environment, TEE）中，确保服务不受到恶意软件的攻击。每次提供上链服务的同时，也会生成证明文件，任何第三方都可以通过该文件，验证整个服务提供过程和结果的有效性。

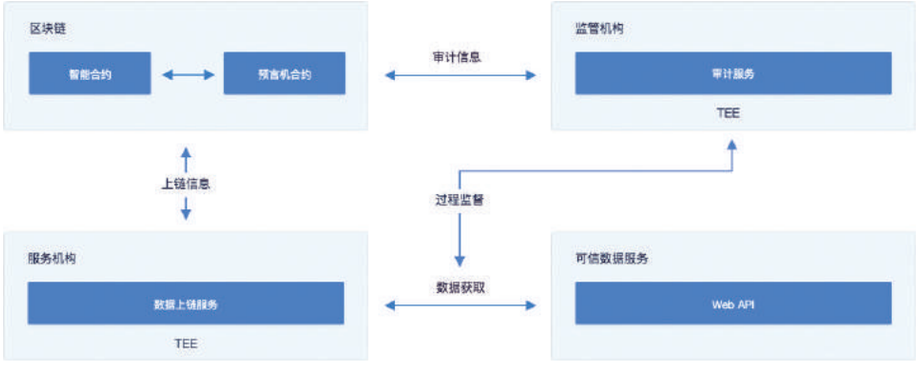


图10 基于预言机的链上链下访问

如图10所示，链上智能合约通过调用预言机合约，获得可信的链外信息。预言机合约获得的上链信息及审计信息，由审计服务和上链服务两个模块共同提供。两个模块共同与可信数据源进行交互，一方负责数据获取，一方负责监督获取过程。

## 5.4 分布式的身份管理

数字身份管理是未来数字经济、数字中国、数字城市的基础，也是区块链应用大规模

应用的必要条件。身份管理是信息系统中不可缺少的功能。在联盟链的区块链系统中，身份管理通常包括两种层面的含义：一是对区块链节点的身份管理（节点身份管理），二是对区块链上业务系统用户的身份管理（用户身份管理）。

对于节点身份管理，通常有两种策略：一种是集中式的身份管理服务，例如基于CA中心（依靠CA中心颁发的数字证书验证节点的身份）、基于VPN网络（在一个VPN网络内运行区块链，利用VPN网络管理机制来控制节点的准入）或基于云平台身份管理（依靠云计算平台自身的用户管理）；另一种是分布式的身份管理服务，完全依靠区块链自身能力来解决节点准入问题。

在分布式的身份管理服务中，核心是对身份信息的管理（主要是管理公钥和公钥的标识符）。可以在区块中存储节点身份信息，也可以在配置中存储节点身份信息。在存储节点身份信息方面，可以采用CA机制，使用一个根证书认证所有节点的方式（例如把根证书信息存在创世区块内，持有通过根证书颁发的子证书的节点可以加入该区块链网络），也可以采用节点身份列表的方式（不使用CA机制，而是单纯的把所有节点的公钥和公钥标识以列表的形式存储起来）。

采用CA机制的分布式身份管理方式，本质上仍然是持有根证书私钥的组织拥有身份管理的权限。我们可以通过拆分私钥，每个组织保存一段的方式，来实现本质上分布式的身份管理。但当发生新组织加入或就组织退出等情况时，对根证书管理是一种技术上的挑战。通常需要更新根证书，重新认证所有节点才能解决实现真正平等安全的分布式身份管理。

在采用节点身份列表的方式中，可以通过预先定义的投票机制或者其他灵活的管理机制来维护整个节点身份列表。这种方式比较符合分布式身份管理原则。

对于区块链上业务系统的用户的身份管理，通常需要根据业务的具体场景，采用针对性的身份管理技术。可以采用集中式的用户身份管理（例如采用某个组织的证书对用户身份进行认证和管理），也可以采用多节点分布式的用户身份管理（例如需要多个组织的证书对用户身份进行认证和管理）。还有一种节点身份管理机制，是和用户身份相结合的。例如在类似DPoS共识机制的系统中，用户可以通过类似选票的Token，选举出超级节点。这种类似的机制在区块链云服务中也可以有对应的实现。

目前，业界另外一种新型的身份管理技术–分布式身份标识（Decentralized Identity，DID）是一种可验证的数字身份形式，具有分布式、自主可控、跨链复用等特点。遵

遁W3C提出的DID设计参考，可以实现基于区块链的分布式身份标识管理，使区块链上的任何实体可自主创建和管理他们自己的身份标识。一个实体可对应多个DID，如图11所示，以满足实体所希望的身份、人物角色和应用场景的分离。这里的实体，可以指现实世界中任意客观存在，并可相互区别的事物，例如个人、组织或具体事物。

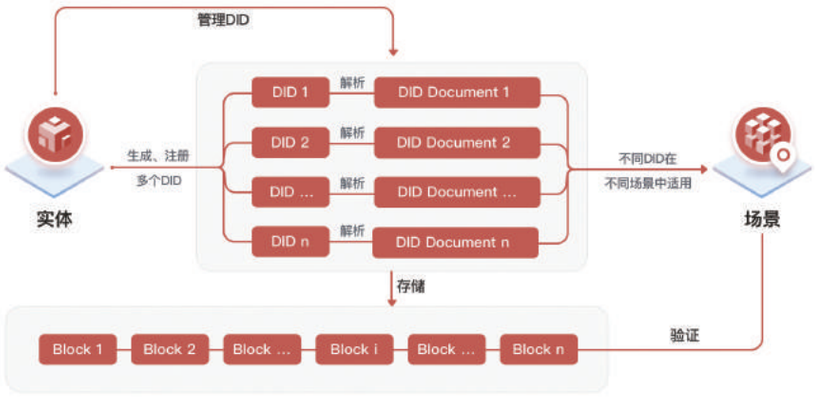


**图11　为实体分配多个DID身份信息上链**

DID是一种去中心化的可验证的数字标识符。它独立于任何中心化的权威机构，可自主完成注册、解析、更新或者撤销操作，无需中心化的登记和授权。DID 具体解析为DID Document。DID Document中主要包含两方面内容：一是加密材料（如公钥、匿名身份识别协议等）；二是属性（包括用于身份验证的信息以及服务端点）。身份验证信息与加密材料可结合提供一套机制，作为DID主体进行身份验证。而服务端点则支持与DID主体的可信交互。

可验证声明（Verifiable Credential）提供了一种规范来描述实体所具有的某些属性。它能表示物理世界中的凭证所能表达的相同信息。DID 持有者，可以通过可验证声明，向其他实体证明自己的某些属性是可信的。同时，结合数字签名和零知识证明等密码学技术，可以使得声明更加安全可信，并进一步保障用户隐私不被侵犯(如图12所示)。

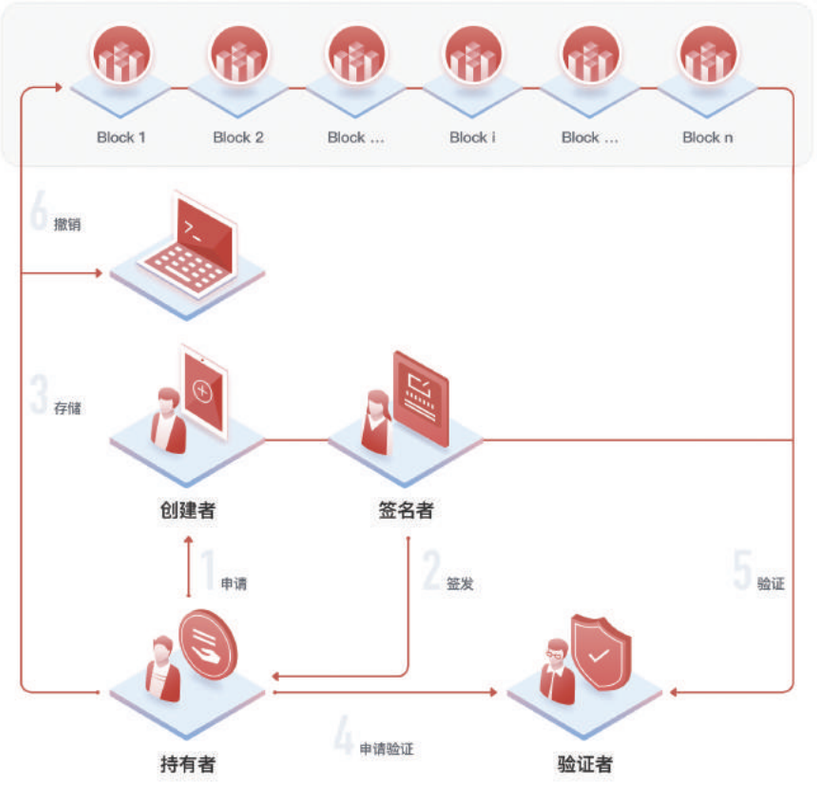


图12　DID信息的验证流程

在现实世界中，认证机构会给一般实体签发可被公众信任的声明，例如车管所给司机颁发的驾照，学校给学生颁发学生证等。而当这些线下的声明被放到网络上进行验证和使用时，可能存在时间延迟、信息被篡改或者隐私信息泄露等问题。因此，通过将标准化的可验证声明放到区块链上，可使其更加便捷、更容易验证、且更加自主可控。进一步加入零知识证明来拓展分布式身份标识的功能，可实现匿名签发可验证声明，或通过验证身份的同时不暴露个人信息，保护用户的隐私信息。

# 6 基于BaaS服务平台的案例分享

## 6.1 供应链金融

供应链金融是贸易金融的一个典型场景，它是指在供应链的业务流程中，以核心企业为依托，运用自偿性贸易融资的方式，对上下游企业提供综合性金融产品和服务。整个供应链金融行业在全球占据级万亿级的市场。在供应链中较大的核心企业因竞争力较强、规模地位强势，往往在交货、价格、账期等贸易条件方面对上下游的中小企业要求苛刻，从而给这些企业造成了巨大的现金流压力。而上下游大多是中小企业，难以从银行融资，结果最后造成其资金链紧张。而供应链金融则为产业供应链上的中小企业提供了一种融资渠道。中小企业持有核心企业的应收账款，以此作为融资资产去向金融机构融资，获得资金后，应收账款变为金融机构的资产，核心企业结算货款时将货款付给金融机构。

目前供应链金融主要是供应链上的企业以应收账款、订单、票据和库存等资产作为担保物，向金融机构进行融资。其风险主要在于融资资产的真实性缺乏保障。有些企业伪造虚假交易，在金融机构进行融资，还有些企业使用同一张发票在多家金融机构骗取资金。对于供应链金融资产真实性的确认,主要依赖于大量人工线下的调查走访审核,效率低下,且不能保证效果,仍然有遭受欺诈的风险。总的来说，供应链金融的行业痛点如下：

一是融资难。由于供应链中的小微企业自身信用级别较低、固定资产等抵押担保品少、经营管理不善、财务信息不透明等原因，难以获得银行等大型金融机构的授信；

二是融资贵。据业内调查显示，一级供应商的年化融资成本通常在6–8%左右，二级供应商的年化融资成本通常在12–18%左右，多级供应商通常面临更高，甚至无资可贷的困境；

三是融资乱。民间借贷利率高企，纠纷不断，一债多抵、一债多卖现象难以杜绝；

四是融资险。供应链由多方主体共同参与，核心企业对供应链上下游的高层级企业掌控有限，信息不对称、不透明甚至传递过程的失真导致供应链运作效率低下，且会引发严重的系统性风险，危害实体经济的发展。

供应链金融场景中的关键需求是——如何存证供应链的关键信息；如何确保可信资质

的评估；如何保障交易各方的权益；供应链的上下游核心企业和供应商之间如何建立互信，降低融资的成本。区块链技术提供的特性和这些需求吻合度很高，数据不可篡改可以让数据很容易追溯，公私钥签名保证不可抵赖，这些机制可以让上下游企业建立互信，区块链中的智能合约可以保障各方约定的合同可以自动执行。基于区块链可信机制的供应链金融解决了供应商单方面数据可信度低、核验成本高的问题，打通企业信贷信息壁垒，解决融资难题，提升供应链金融效率，通过供应链中各方协商好的智能合约可以让业务流程自动执行，资金的流转更加透明，极大提供公平性。

在如下的大大买钢网案例中，大大买钢网是一家垂直互联网电商。我们都知道大宗商品交易，天然的占用资金大，钢铁产业链上真正需要钱的人，是在流通环节中的钢材贸易商。他们的金融需求是最大的，但是他们作为小微企业，天然是信用不强、担保能力不强的，很难获得融资。在图13场景中，下游客户王总通过大大买钢网下了10吨钢材的订单，大大买钢网通过第三方仓储进行出库，第三方仓储安排物流进行运输，最终达到了下游客户王总。在这个多方协作的过程中，出库单、运输单、签收单充当着信用传递和数据传递的媒介，任何一个环节出现了不可信的问题，都会对整个供应链造成风险。


图13　供应链金融应用场景

我们借助区块链共同记账和不可篡改的特性，首先打通各个环节各个参与方系统的数据壁垒，让每一个参与方都在区块链上进行数据的协作，进而在一个可信的环境下，提高商家的协作效率。大大买钢网通过更新订单合约中的订单状态，订单状态的变化就会自动触发出库这个操作；第三方仓储基于可信的出库信息，在物流合约上，通知物流取货运输；第三方物流公司根据要求，按时送达到客户手中；下游客户王总，可以通过区块链，实时查看订单状态，同时签收信息，也通过区块链反馈给大大买钢网。

在区块链的交易过程中，大大买钢网对下游客户王总的应收账款，经过区块链的背

书，以及参与方的背书，就会变成可信的应收账款资产。借助于我们的供应链金融平台，就可以为大大买钢网提供相应的金融服务，缓解资金流压力。

## 6.2 版权确权

传统的版权登记方式，耗时往往很长。网络时代的数字作品具有产量高、传播快的特点，经过登记再发布早已经丧失了内容的时效性。而且每次登记动辄费用上千，这就造成了大多数网络作者并不进行版权登记和保护，导致侵权频发。在抄袭行为被发现后，往往要求原创作者拿出侵权证据，在作品未进行登记与保护的情况下，获取具有法律效力的证据更是难上加难。

在实际维权过程中，原创作者往往面临两难处境：内容分发平台的维权渠道手续复杂且效率不高，通过法律渠道进行诉讼的成本更高。导致大多数原创作者维权无门，只能选择沉默，任由权利被侵犯。对互联网环境中的原创作者来说，能为其带来最大价值的是原创凭证和维权依据。针对作品的传播及交易需求，他们需要更加便捷、安全、可信、价格低廉的版权保护方式。从这个层面来讲，区块链的特性完美地满足了上述需求。

基于区块链存证的版权解决方案具有可定权、可溯源、不可篡改等特点。通过区块链版权保护平台，只需完成上传文件、确定作者、填写相关登记信息等简单几步操作，即可进行版权登记。在线生成的版权登记证书拥有区块链上唯一且可追溯的定权哈希和符合《电子签名法》的时间戳。一旦通过区块链技术完成了版权存证，即可联网查询版权登记信息，永久有效，无法篡改（如图14所示）。 区块链版权服务通常包含版权存证、版权检测追踪、侵权取证三个部分：

1) 版权存证

√ 选择文件、获取数据指纹：选择需要存证的文件，通过哈希算法计算出该文件和关联信息的数据指纹。

√ 数据写入区块链：在用户确认后，系统将得到的数据指纹写入区块链中，一经写入便无法篡改。

√ 获取存证结果：根据用户需求生成存在证书供用户保留，也可根据用户需求，提供纸质书面报告。

√ 数字指纹验证：根据客户需求，在用户需要对存证的指纹进行验证时，提供数字指纹比对查询。


图14　版权存证上链流程

2)　版权检测追踪

√ 作品哈希生成：针对参与登记的版权作品，生成唯一的哈希值，并将其在联盟链上进行登记。

√ 全网检测：提供重点网站自动化爬虫，将监测到的内容与作品进行匹配，相似度达到阈值自动进行侵权预取证操作。

√ 侵权匹配：对已进行侵权预取证的内容进行持续追踪及进一步分析匹配，待确认侵权则直接进行侵权取证。

3) 侵权存证

√ 侵权取证：当发现侵权行为时，快速调用版权服务中的侵权取证接口，对侵权网站进行页面抓取取证，并将取证结果保存在联盟链中；系统对侵权URL地址进行域名解析，通过预言机服务将URL对应的侵权内容进行存储，并生成可供第三方检测的存证过程合理性证据，将侵权行为固化为证据进行保存；固化后的证据保存在区块链中，数据永久存储且不可篡改，符合法律对电子证据的要求。

√ 侵权追踪：对于已进行侵权存证操作的侵权内容，版权服务提供持续性的侵权监控、侵权追踪等服务，确保侵权方对于侵权内容采取相应处理。


图15　基于区块链系统的侵权检测流程

在区块链存证系统中，在上传信息到拿到版权证书的同时，区块链版权存证服务将用户提交的申请人、作者、作品内容、存证时间等相关登记信息进行密码学处理，将其数据指纹上传至区块链网络中，完成区块链存证。通过引入公证处、版权局、知名高校作为版权存证联盟链的存证和监管节点，所有上链的版权存证信息都会经过多个节点的验证和监管，保证任何时刻均可出具具备国家承认的公证证明，具有最高司法效力。同时，通过在公证处部署联盟链存证节点服务器，存证主体即可视为公证处。在遭遇侵权行为时，区块链版权登记证书可作为证据证明版权归属，得到法院的采信（如图15所示）。

## 6.3　积分兑换

积分是会员忠诚度计划的一部分，在金融服务、旅游、零售等行业被广泛使用。然而，积分系统和兑换方式在不同的积分发行人之间形成天然隔离，在不同的积分系统之间实现积分兑换变得异常繁琐。

基于区块链技术的积分联盟方案为公司带来统一的积分兑换系统，可以使公司专注在维护客户忠诚度积分计划，而不会增加客户原有积分系统的复杂性。积分联盟方案接入不同的本地合作伙伴，消费者有了更多的积分兑换选择，客户获取更多的个性化产品以及积分相关的一站式服务。另一方面，积分联盟方案提供通用的积分清结算服务，支持多家公司共同记账、实时清算、定期结算。积分联盟方案提供两种不同的积分兑换方案。不同厂商的积分可以通过统一积分实现积分的通用兑换，也可以通过设置不同汇率实现积分之间的两两兑换。

BaaS平台帮助积分联盟方案的参与方实现区块链网络与节点的部署与运维，更重要

的，BaaS平台管理和维护积分联盟方案中不同类型的智能合约，包括如图16所示的积分生成、积分兑换、积分转让、积分清算等。

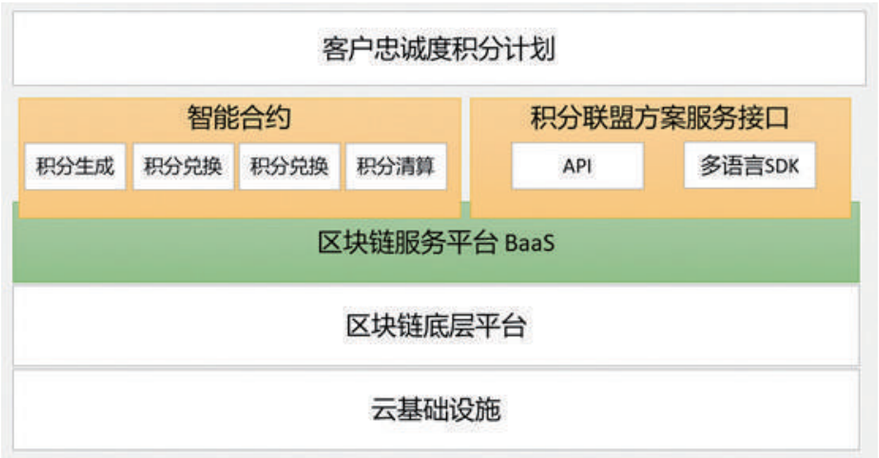


图16　基于区块链的商家积分兑换系统

## 6.4　产品溯源

产品溯源，是一种追溯根源行为，通常是指物品或者信息在生产、流通及传输的过程中，利用各种采集和留存方式，获得物品或者信息的关键数据，如流通和传输的起点、节点、终点，数据类别，数据详情，数据采集人，数据采集时间，并通过一定的方式，把数据按照一定的格式和方式进行存储。通过正向、逆向、定向方式查询存储的相关数据，就可以对物品及信息进行追溯根源。

产品在人们生活中主要是为人们提供各种衣食住行方面的需求，在人们的生活经济中有着重要的地位和作用，比如促进相关行业和产业的经济和文化发展等。但是在传统的产品行业里，产业链非常长，从原材料到成品，中间历经多个环节，这些环节大多都是割裂、无序的，产品到达最终使用者的手中之后，中间的过程大多无法得知，无法追溯。加之现在出现的许多假冒伪劣商品，导致消费者对于现在的产品尤其是食品持怀疑态度。而且同样的产品由于各种方式的包装，导致价格不一，高低差距很大，人们不知道如何抉择，不了解那个食品提供的信息是真实可靠的。在生态农业建设中还有更多深层的问题，比如说供需不平衡等。

溯源的示例系统如图17所示的农场溯源平台架构，区块链技术在整个农场溯源平台架构中处于底层，整体业务架构中还可嵌入实时计算、大数据处理、人工智能等模块。此外，由于农场将会产生巨大的数据量以及并发数据，必须有高效的实时计算和大数据平台

来承载对接IoT，而为了让用户更好地认知整个溯源历史，同时在大数据的基础上做了数据可视化等。

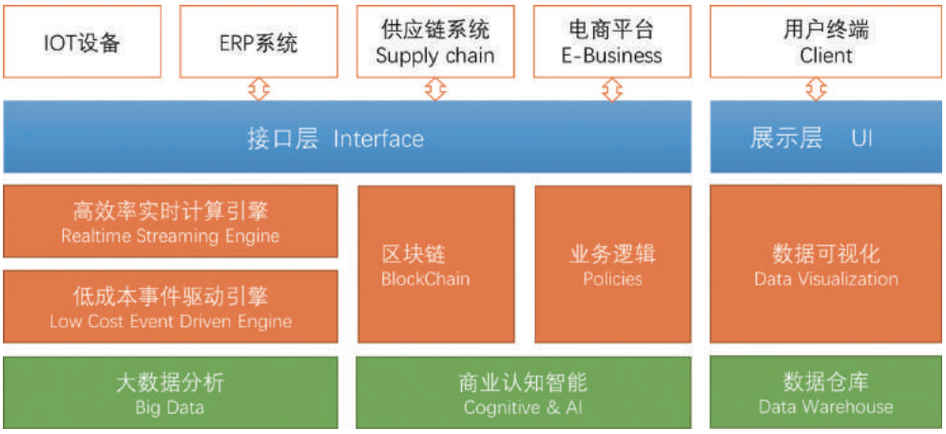


图17　基于区块链的农场溯源平台

为了满足各种来源的数据进行上链，溯源平台设计可以支持多种数据源的上链，可以是离线数据，也可以是IoT设备的数据，也可以是来自其他业务系统的数据等。通过定义数据规范和适配业务字段的变化，对上链的数据进行建模，制定数据上链标准，实现上链数据项的灵活配置。该溯源系统可以横向扩展支持多种行业的产品溯源，如农业产品、工业产品等。

基于区块链的农场溯源系统的价值主要体现在如下方面:

1)　全流程的关键业务数据上链，做到信息公开透明

把区块链技术应用到从种植品种选择开始到最后送到消费者手中的所有环节中，大的环节包括粮食种植、粮食收割、粮食加工、粮食仓储、粮食运输等。每个环节都有很多细分的过程，每一个过程产生的数据都会记录在区块链的账本数据中，智能合约内部逻辑会实现每个过程数据之间的关联性，最终生成一个唯一的粮食身份证。物联网数据直接上链，提供真实的第一手数据。

2)　链上链下结合，确保信息真实的情况下还能保证品质

农场溯源系统涉及到物联网设备采集标准，作业电子表单，种植标准，风险点阈值，包括细节字段和关键节点，这些流程和标准规范化链下的粮食生产过程，提升每个步骤产出的质量，包括链下粮食生产的质量，也保证了上链粮食数据的品质。

3)　海量数据存储优化确保系统稳定运行

农场溯源系统可以管理上万亩土地，部署在土地里的物联网设备实时收集不同类型的数据，不同农时作业时产生的数据也会实时上链，产生了海量的数据，存储到大农场平台的数据仓库。

4) 智能合约让种植生产流程良性循环

区块链整合了不可篡改的种植和销售的各种数据，在这些数据基础上实现的智能合约能够反馈销售结果到种植环节。优良的粮食品质能够给种植这些粮食的农户带来更好的收益，对改进粮食种植有积极的作用，也能在农资贷款等提供数据的支撑，促进粮食种植的良性循环。

5) 共识机制确保数据的一致性并且不可篡改

农场溯源系统底层的区块链技术实现的共识机制包括交易背书、交易排序、交易验证记账等多个步骤，每个步骤都需要对请求进行签名和验证。只有多个背书节点对交易结果进行背书，满足了背书策略，并且在排序服务节点之间达成共识，排序产生的区块经过记账节点验证通过后，才能记录到账本中。任何一个步骤出现错误都会导致交易失败，经过这些步骤后每个记账节点记录的账本都是一致的。农场溯源系统基于PKI体系验证用户的身份，对提交请求进行数字签名的验证，保证数据的安全性和不可篡改性，让数据更加透明，大大提高消费者信任度。

## 6.5 游戏

区块链作为一种新技术，我们认为在真实游戏场景里应该有更大价值空间，能够在游戏的真实性、透明性、稀缺数字资产的唯一性方面发挥巨大作用。游戏产业绝大多数环节都是纯数字化的、虚拟化的。游戏世界原本就存在用户社群、虚拟商品交易、代币结算，这些都与区块链应用的很多要素不谋而合。

基于区块链的游戏行业可在通过以下六个方面，将区块链融入现有游戏进程，解决传统游戏的问题：

1) 数据可信任。通过区块链账本多节点记录独一无二的线上数字藏品，虚拟道具内容、数量、抽取概率等核心数据存储于区块链上，游戏运营方无法滥发游戏商品和道具。使游戏数据透明，可信任，减少由于运营商和玩家间的权力不平等带来的各种矛盾和纠纷。

2) 游戏道具确权。作为多媒体技术产品中最复杂的集合体，游戏道具集美术、文字、代码于一身。游戏中的虚拟物品也成为玩家最重视的元素之一。区块链可为游戏道具

的权利流转提供了安全可控的存储方式。基于网游企业的研发设计，在允许道具交易的游戏中，买、卖行为变得难以篡改，在保障交易安全的同时，也为玩家持有虚拟财产、数字藏品提供了可能。

3) 区块链道具在游戏中的实际作用。接入区块链的游戏道具在游戏进程中会有推动游戏进展的作用。例如，在游戏《一起来捉妖》中玩家在游戏带上某只专属猫进入战斗时，全员会增加某部分属性，从而可能更容易赢得战斗。

4) 通过区块链账本实现游戏进程中的传承与永久记载。游戏道具资产一旦上链，转移、拆分、提现等操作都会通过账户公私钥严格控制起来，并且所有的操作都会有签名校验，交易双方都会留下痕迹。游戏道具的传承将被永久保存记录下来，为玩家和数字藏品建立充分的情感连接，让这份藏品在未来的无论哪个时刻，都可以由玩家在区块链上调取、交互，让它成为玩家永恒的记忆。

5) 安全保护。用户的虚拟藏品存储在多节点记账的区块链上。就算游戏运营方数据库被入侵，也不会造成用户游戏财产的丢失或盗用。

6) 媒体节点的引入。“媒体节点”指架设在媒体机构的观察节点，为观察节点（observer node）其中一种，不参与记账及共识，但拥有账本读取权限的节点。基于区块链的游戏系统可把观察者节点给予媒体，对于有责任感的媒体而言，他们代表了社会大众，对游戏资产是否公正、超发进行监督。

# 7 结束语

随着区块链的推广普及，越来越多的企业认识到区块链的商业价值并开始探索应用到自身业务中。但是企业在使用区块链的过程中，也常常遇到技术门槛太高、安装部署复杂、管理运维成本高等痛点。

区块链服务平台为企业提供区块链基础设施和服务，解决企业使用区块链的各种痛点，加快了企业区块链业务的落地速度。因此区块链服务平台得到了越来越多的重视，很多有实力的厂商也纷纷推出各种区块链服务平台产品。

本白皮书总结概述了常见区块链服务平台的架构、功能、底层技术以及应用案例，希望读者借此更好地了解区块链服务平台的作用，更好地应用到企业区块链业务实施过程中，同时为企业级区块链生态建设的不断推进助一臂之力。

**可信区块链推进计划**

地址：北京市海淀区花园北路52号　邮政编码：100191

联系电话：010-62300249　传真：010-62304980

网址：www.trustedblockchain.cn