

# 荣泽企业级区块链平台管理软件 (RBaaS) 产品白皮书

## 目录

1. 前言	2
2. 产品概述	4
2.1 区块链技术背景	4
2.2 企业级区块链	4
2.3 产品定位	5
2.4 产品优势	6
2.5 产品荣誉	7
3. 产品架构及功能	7
3.1 产品架构	8
3.2 产品功能	8
3.2.1 区块链服务	8
3.2.2 区块链管理	10
3.2.3 合约管理	11
3.2.4 可视化账本结构	12
3.2.5 分布式数字身份	13
3.2.6 运维管理	14
3.2.7 安全与隐私保护	15
4. 产品应用领域	15
4.1 政务领域	15
4.2 金融领域	15
4.3 公共服务领域	16
4.4 供应链领域	16
4.5 物联网领域	16
4.6 医疗领域	16
4.7 数字版权领域	16
4.8 公益领域	17
4.9 数据服务与共享	17

## 1. 前言

2019年10月24日，中共中央政治局首次就区块链技术发展现状和趋势进行集体学习。会上习近平总书记在主持学习时发表了讲话。他指出，区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域。目前，全球主要国家都在加快布局区块链技术发展。我国在区块链领域拥有良好基础，要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展。最后，习近平用四个“要”为区块链技术如何给社会发展带来实质变化指明方向。

(1) 要探索“区块链+”在民生领域的运用，积极推动区块链技术在教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域应用。

(2) 要推动区块链底层技术服务和新型智慧城市建设相结合，探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理智能化、精准化水平。

(3) 要利用区块链技术促进城市间在信息、资金、人才、征信等方面更大规模的互联互通，保障生产要素在区域内有序高效流动。

(4) 要探索利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，深化“最多跑一次”改革，为人民群众带来更好的政务服务体验。

区块链技术有着去中心化、点对点传输、规则透明、可追踪、不可篡改、数据安全等特点，可以建立一套公正、透明、可信的规则。区块链技术具备一种“降低成本”的强大能力，能简化流程，降低不必要的交易成本及制度性成本，可以有效提高运营效率，为经济增长注入活力。

区块链技术具有使能作用，结合5G、物联网对现实世界数据的采集，以及搭建人工智能算法的自动交易和激励系统，有望在未来形成一套无人值守的价值数据交换和交易体系，将人类社会带向数字化的信任经济时代。区块链应用最突出的优势表现为以下两个方面：

交易支持方面，得益于上链数据本身具备多个交易主体相互背书和相互校验的特质，基于区块链智能合约等多种模式的商业交易可以大幅降低数据核实的环节和成本，同时又能保证商业交易的风险降低，交易更具确定性。传统中心化的交易方式将随之发生改变，数据和价值的传递或转移将变得更为顺畅。

数据共享方面，区块链技术其本身具备的分布式数据存储、点对点传输、加密算法、防篡改与保护隐私、智能合约等核心特征。基于这些特征，部署跨主体间的联盟链，用区块链技术搭建一张全社会的共享数据网络，以技术手段来解决跨主体的信任问题。

随着区块链技术的发展和广泛应用，涌现出了像以太坊、超级账本等区块链平台，催生了大量业务场景。但是对于普通用户来说，由于缺乏区块链的系统知识和研发经验，对于如何选择区块链底层平台，研发适合自己业务场景的区块链应用往往有较大困惑。区块链即服务（Block chain 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。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。

荣泽科技在区块链技术的创新与实践过程中，逐渐认知到区块链并不单纯是一种技术，而是一种思维方式的变革，是一种社会化的“共识信任”理念，而推广这一理念不能依靠一家之力。因此荣泽科技聚集核心研发力量，倾力打造荣泽区块链云服务平台（RBaaS），期待携手合作伙伴共建区块链技术生态，落地更多的区块链“杀手锏”级应用。

荣泽科技愿意全面开放自身的区块链技术积累，与您互利共赢、共创未来！

## 2. 产品概述

### 2.1 区块链技术背景

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）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。

### 2.2 企业级区块链

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。安全可信是区块链的核心要求,标准规范性日趋显得重要。

经过多年的企业级区块链应用系统研发实践和成功经验,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。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。

区块链的核心价值在于构建可信任的多中心体系,有潜力成为构建价值互联网的基础设施。荣泽科技致力于打造企业级区块链产品并提供行业解决方案,开发出了高性能、高可扩展的区块链基础产品,具备快速构建上层应用业务的能力,满足大规模用户数量的应用场景。

瞄准企业级产品化运营能力,荣泽区块链基础产品已取得多项技术突破和创新,在性能、扩展性、安全和运维等方面形成一系列技术特色和优势。在与产业合作伙伴共同深入探索区块链应用场景的基础上,荣泽区块链已应用于政务服务、数字资产、贸易金融、商业联盟、股权债券、供应链溯源、联合征信、公示公证、物联网共享、数据安全等领域。以多中心化信任为核心,打造新一代价值流通网络,让数字资产都自由流动起来。

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。

### 2.3 产品定位

RBaaS 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。

RBaaS 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。

RBaaS 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应用。

## 2.4 产品优势

### ①. 技术优势

荣泽科技具有全国领先的技术创新能力，底层技术平台 RBC 自主研发并获取了专利。融合了并行计算技术，将区块链计算性能提升了 30%。优化了 BFT/RAFT 共识算法，可满足不同信任环境下对安全和隐私的需求。

### ②. 安全优势

全面支持国产化和自主知识产权，兼容国产芯片（ARM、X86 等）、兼容国产操作系统（麒麟、统信 UOS 等）、兼容国产云计算（华为云、金山云、阿里云等）。支持 SM2 等国密算法、同态加密、行/列级数据隐私保护。支持权威机构颁发的数字证书，提供区块链创始块的安全方案。提供智能合约安全沙箱，可实现分级分层的智能合约安全执行环境。

### ③. 性能优势

通过深层次系统优化，荣泽区块链平台已具备快速交易验证、海量存储等性能优势，标准环境下每秒交易高达 10000TPS。

### ④. 运维优势

支持全平台部署，荣泽区块链技术平台（RBC）的所有代码均可跨平台编译运行，平台相关代码均封装成基础库，业务逻辑可以实现在云平台上快速部署。提供运维管理所需的可视化工具。提供区块链 API 接口，供这些场景相关的业务直接使用。在新的业务场景下，荣泽区块链技术平台（RBC）可以基于现有的框架为用户快速定制接口，满足业务功能需求。同时提供已封装的 SDK 软件开发包。

### ⑤. 易用性优势

提供可视化账本结构设计器、智能合约部署/比较工具，大幅降低应用系统开发的技术门槛，并显著提升开发效率。

### 2.5 产品荣誉



上图：通过工信部可信区块链功能、性能和安全测试

**国家互联网信息办公室关于发布第三批境内区块链信息服务备案编号的公告**

2020年04月24日 17:00 来源：中国网信网

2019年2月15日《区块链信息服务管理规定》（以下简称《管理规定》）正式实施以来，国家互联网信息办公室依法依规组织开展备案审核工作，已发布2批次共506个境内区块链信息服务名称及备案编号，现发布第三批共224个境内区块链信息服务名称及备案编号。任何单位或个人如有异议，请于即日起10个工作日内将相关意见通过电子邮件发送至bc\_beian@cert.org.cn，或邮寄至北京市朝阳区裕民路甲3号国家互联网应急中心，邮编：100029（信封上注明“备案公告反馈”）。提出异议应以事实为依据，并提供相关证明材料。

根据《管理规定》要求，区块链信息服务提供者应当在其对外提供服务的互联网网站、应用程序等显著位置标明其备案编号。备案仅是对主体区块链信息服务相关情况的登记，不代表对其机构、产品和服务的认可，任何机构和个人不得用于任何商业目的。网信部门后续将会同各有关部门，依据《管理规定》对备案主体进行监督检查，并督促未备案主体尽快履行备案义务。请尚未履行备案手续的相关机构和个人尽快申请备案。

**附件：境内区块链信息服务备案清单（第三批）**

108	江苏荣泽信息科技股份有限公司	江苏省-南京市-浦口区	荣泽区块链云服务平台 (RBaaS)	苏网信备 32011120598288700074 号
-----	----------------	-------------	--------------------	-----------------------------

上图：通过国家网信办第三批境内区块链信息服务备案

### 3. 产品架构及功能

荣泽区块链云服务平台（RBaaS）旨在建立与维护可运营、可管理、易用的区块链网络，并帮助工程师快速开发区块链应用。

RBaaS 为运维工程师提供建链工具以及节点基础监控和业务监控服务，并通过告警服务在节点故障及时通知到运维工程师，以便将故障响应时间最小化，提高运维工程师的运维管理效率。

RBaaS 使不同经验水平的开发人员可以通过可视化界面，使用组件和模型驱动的逻辑来创建、测试和部署各种区块链业务模型、智能合约以及应用。提供一系列的区块链基础服务、模型设计器帮助开发人员在“零区块链基础”知识的背景下快速开发区块链应用。

### 3.1 产品架构

荣泽区块链云服务平台 (RBaaS) 的功能如下图所示，主要包括区块链服务、区块链管理、合约管理、可视化账本结构、分布式数字身份、运维管理六大部分。



上图：产品架构

技术平台支持荣泽自主知识产权的区块链技术平台 (RBC)，同时还支持 Fabric 1.4、FISCO 2.x 等国内外主流区块链技术平台，并且会根据业务场景的需求不断扩充支持的区块技术平台类型。

区块链服务包括：加解密服务、CA 证书服务、数据授权、数据上链服务。

区块链管理包括：多链多通道管理、组织/联盟管理、主机资源管理、应用管理。

合约管理包括：合约安装/部署/审批等全生命周期管理、合约比较、合约测试执行。

可视化账本结构（业务模型）包括：模型库及模型表管理、数据权限管理、索引管理、模型数据在隐私保护的前提下的查看及修改。

分布式数字身份包括：身份标识符管理、凭证发行方管理、凭证使用方管理、凭证模板及凭证管理。

运维管理包括：链浏览器、快速自动化部署、监控与告警、可视化看板。

另外 RBaaS 还通过多层多重的安全措施保障数据的安全、保护用户的隐私。

### 3.2 产品功能

#### 3.2.1 区块链服务

##### 3.2.1.1 加解密服务

加密、解密服务为用户的上链数据提供隐私保护机制。用户在设计可视化账本结构（业务模型）时选择加密，则该业务模型的数据上链时自动加密，在用户查询时根据数据所有者授权解密，非授权用户无法查询，直接查询区块数据得到的也是密文，从而保障了用户的隐私数据不被泄漏。

### 3.2.1.2 证书服务

在区块链技术的公私钥体系下，证书服务负责：公私钥生成，公钥写入，私钥签名与管理；保存应用层用户信息与区块链地址映射关系；支持实名认证及审计的监管需求。为应用适配层提供两类接口：非托管型接口和托管型接口。

#### ①. 非托管型接口

适合有能力在应用端实现安全级别较高的私钥生成和使用的企业机构。例如，在金融领域，将私钥的生成与管理跟现有的U盾、电子签名等安全的客户端体系相结合。

#### ②. 托管型接口

适用于互联网化程度较高的应用场景。公私钥直接作为用户名和密码使用对普通用户来说识记成本高体验差，大多数用户习惯用手机号、邮箱、昵称等作为用户名。因此，在托管型接口里，通过安全的私钥生成与管理的体系，应用层用户信息与区块链地址映射，使上层应用和底层区块链平台都无法触碰到用户的私钥。

### 3.2.1.3 数据授权服务

通过授权服务实现模型库级、模型表级、表字段级、行级等精细化的访问控制。被授权的主体可以是组织，也可以是组织的成员，并且与数字身份相结合，为每个组织、组织的每个成员分配唯一数字身份标识符。同时授权数据保存在区块链账本中，保障不会被篡改并且全程可追溯；授权逻辑通过智能合约实现，在安全沙箱中运行，保证了授权过程的安全。

数据授权服务保障了数据的安全与隐私，同时也为数据的跨组织、跨链共享提供了基础能力。

### 3.2.1.4 数据上链服务

针对区块链应用开发门槛高、难度大的问题，平台提供多种数据上链服务，屏蔽了区块链底层技术细节，降低了区块链开发难度。

1、平台提供可视化的账本结构设计器，用户无需开发智能合约即可完成账本结构的设计。

2、平台将对账本数据的访问封装成通用的协议，用户直接通过 API 即可实现账本数据的读写，无需自行开发实现区块链客户端。

3、平台提供 WEB 界面访问账本数据，通过可视化界面即可完成数据上链、上链数据查看、追溯数据历史。

### 3.2.2 区块链管理

RBaaS 可以帮助政企用户快速构建稳定、安全的区块链开发、测试、生产环境，大幅减少区块链部署、运维、管理的难度，提高区块链运维的效率。

平台提供了联盟链创建和管理、链浏览器等区块链管理功能，同时还提供了通道成员管理、业务模型管理、合约管理与审批等通道和智能合约管理功能。

#### 3.2.2.1 多链多通道管理

RBaaS 支持一套平台管理多个区块链网络、多个通道。多链多通道管理包括以下子功能。

##### (1) 创建区块链

创建区块链指企业采购荣泽区块链一体机或者自主提供服务器资源，快速进行区块链部署。区块链创建成功后可进行创建通道、添加联盟成员等后续工作。

##### (2) 创建通道

通道 (channel)：区块链专业术语，用于实现区块链中业务的隔离。每个通道可代表一项业务，联盟内的全部或部分成员作为业务的参与方加入到通道，成为通道的成员。一个区块链可以有多个通道，每个通道可视为一条子链，对应一套账本。

创建通道指在区块链上创建一个子链，选择区块链的全部或部分节点作为记账节点，每个通道使用独立的账本。

##### (3) 添加新组织 (联盟成员)

当有新成员加入联盟时，需要使用此功能添加联盟成员。有两种方式添加成员：自行添加新成员、链管理员添加成员。两种方式无本质区别，只是管理方式的不同。

自行添加新成员：首先链管理员向受邀机构发送邀请码，受邀机构登录平台填写邀请码，自行完成新成员的添加。

链管理员添加成员：由链管理员在平台上新增联盟成员。

新组织加入到区块链后，还需要加入到通道才能参与相应通道的业务。

#### 3.2.2.2 主机资源管理

管理自动化部署区块链网络所需的主机资源，RBaaS 按照用户配置的参数自动在该主机上部署区块链网络。RBaaS 支持 Docker 及 Kubernetes (K8S) 类型的主机资源。

#### 3.2.2.3 组织管理

组织 (联盟成员) 可以选择加入通道，在得到该通道多数成员 (>1/2) 同意后即可成功加入，加入通道后才能参与该通道的相关业务 (执行智能合约、为数据上链背书等)。

同样联盟成员也可以选择退出通道，在在得到该通道多数成员 (>1/2) 同意

后即可成功退出，退出通道后将不能参与该通道的相关业务（执行智能合约、为数据上链背书等）。

### 3.2.2.4 应用管理

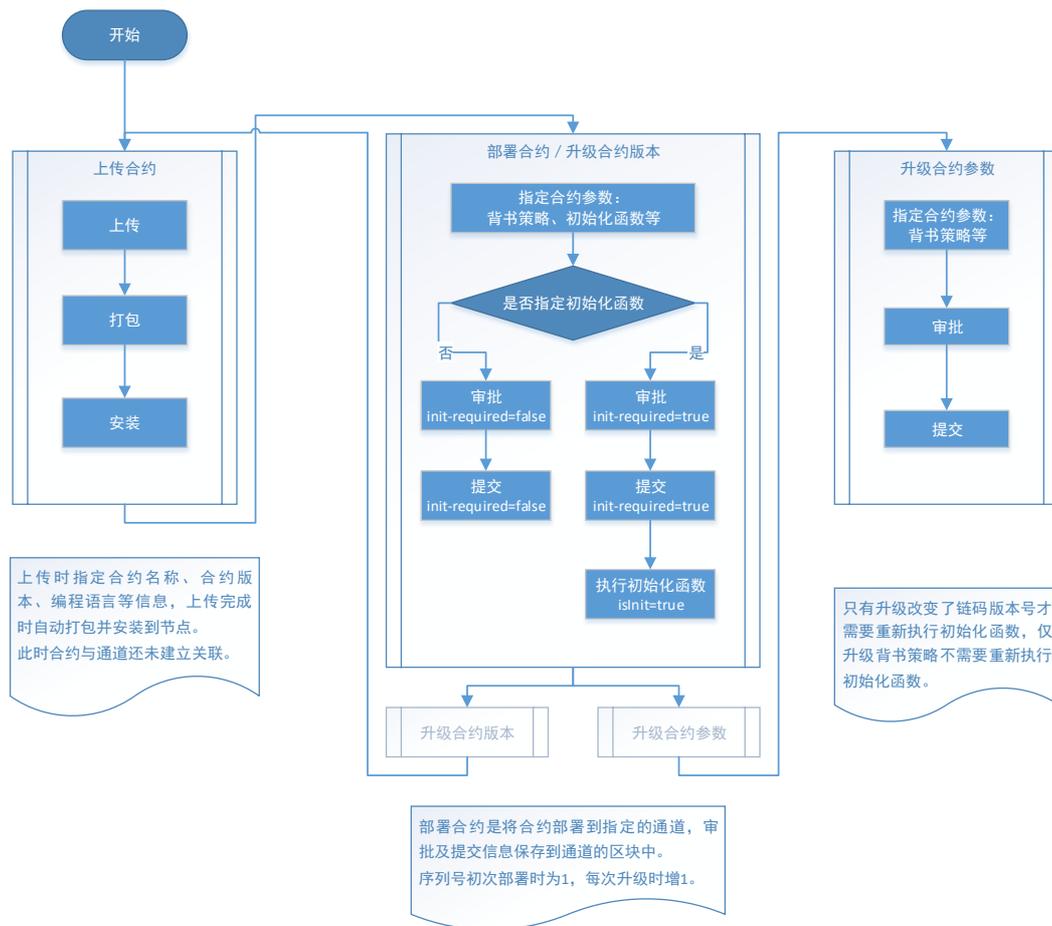
RBaaS 除了提供区块链基础服务外，还提供了一些基础应用，例如：跨链网关、预言机网关、数字身份等。并且提供了扩展机制，方便用户添加、发布自己的应用。

### 3.2.3 合约管理

智能合约，又称为链码，是用计算机语言描述合同条款、交易的规则等，通过调用智能合约实现交易的执行和对账本数据的操作。

平台支持 Java、Go Lang、Node.js 作为智能合约开发语言，减少了开发人员的学习成本。智能合约运行在安全沙箱中，无法访问沙箱外部的资源，这样保证了智能合约的安全性。通过 Web IDE，开发人员无需安装任何工具即可使用，支持智能合约的在线查看、比较、下载与升级。

RBaaS 为智能合约全生命周期管理提供可视化工具，RBC 2.4 智能合约生命周期如下图所示：



上图：RBC2.4 智能合约生命周期

### 3.2.3.1 合约上传/部署

智能合约上传是指将开发完成的智能合约打包、安装到区块链网络的各节点。上传时指定合约命名、合约开发语言、合约版本等信息。

智能合约部署/升级是指将已安装的智能部署到指定的通道，部署时指定部署的通道、合约背书策略、合约初始化函数名称、初始化函数参数等。

如果已经存在同名的智能合约，则升级该智能合约，可以升级智能合约版本，也可仅升级智能合约背书策略等参数：当智能合约代码修改时，需要重新上传并升级版本；如果仅修改了背书策略，可以仅升级参数。为了保护联盟各方利益，提高交易的安全，智能合约部署或升级时，必须经联盟成员审批通过并提交后才能生效。

### 3.2.3.2 合约审批

智能合约定义合同条款、交易规则等并且由各成员执行，为了保护联盟各方利益，在智能合约部署或升级时必须经联盟成员审批通过才能生效。同时，智能合约的所有变更及审批过程全部记录到区块链账本上，以便责任追溯与审计。

### 3.2.3.3 合约比较

平台提供了智能合约比较功能，将待审批的智能合约版本与当前运行的智能合约源代码一对一比较，联盟成员可清楚知道合约做了哪些修改，审批也更加方便。

### 3.2.3.4 合约执行

用户可以直接在 RBaaS 上测试、执行智能合约，执行时需要指定操作类型（invoke 或 query）、执行的函数名称、函数需要的参数。

**【注】**操作类型为 invoke 才会修改账本数据；query 仅能查询数据。

### 3.2.3.5 合约查看/下载

联盟成员可以查看当前的智能合约信息，如版本号、发布时间等。平台可在无需安装任何 IDE 工具的情况下查看智能合约的源代码，也可以将整个合约源代码下载到本地。

### 3.2.3.6 合约版本管理

平台支持智能合约的版本管理，每次上传/升级智能合约时必须指定版本号。同时还可以查看历史版本信息，查看或下载历史版本智能合约的源代码。

## 3.2.4 可视化账本结构

平台提供可视化的界面来设计区块链账本结构（业务模型：即对区块链上以键值对 (Key, Value) 存在的信息以结构化方式进行定义和可视化展现的技术），将区块链账本抽象成模型库、模型表、表字段，表字段支持字段类型、字段长度、是否允许为空、是否为主键等属性。同时模型表可以创建索引，支持多个字段组合索引。通过该设计器，开发人员无需了解区块链技术细节，即可像设计数据库

表结构一样轻松设计区块链账本结构。

#### 3.2.4.1 模型库及模型表

平台提供可视界面对业务模型库、模型表、表字段、索引进行增加、修改、删除、查看功能。

经过授权可将业务模型（账本结构）从某区块链导出，再通过导入功能部署到其他区块链，这样做便于多链的业务协同，也便于将业务模型从开发环境迁移到测试、生产环境。

#### 3.2.4.2 模型权限管理

用户可以设置业务模型的访问权限，被授权对象为联盟成员（群组）或单个账户。可以针对模型库、模型表整体授权、也可对表字段读、写权限单独授权。

同时还支持数据的行级访问控制，控制参数可以为：数据上传者可访问、数据上传者所属组织可访问、不控制（即本通道所有组织可访问）。

#### 3.2.4.3 模型数据

为了方便开发人员开发、测试业务模型以及运维人员定位、解决问题，平台提供模型数据增加、删除、修改、查询功能，用户直接以可视化二维表的方式查看、修改模型数据。

#### 3.2.4.4 数据历史

为了方便对数据进行追溯与审计，平台还提供数据历史功能，可以追溯数据从诞生以来的所有变更历史。历史信息包括：交易 ID、变更时间以及历史数据值，通过交易 ID 可以查询该历史的区块及交易详细信息。

### 3.2.5 分布式数字身份

基于区块链技术建立符合 W3C 标准的分布式数字身份平台，为主体和抽象主体提供唯一标识以及可验证的数字凭证。通过创新数据的连接方式，保证了数据的自主可控，保护了主体的隐私和合法权益，符合数据要素市场化的发展趋势。经过主体授权使用标识可串联不同系统、链，也可实现数据的高效汇聚。

同时，数字身份平台通过一系列可插拔的适配器，将传统权威凭证发行机构的接口服务转换成可验证的凭证，为政企用户（凭证应用方）提供统一、规范化的凭证验证服务。

#### 3.2.5.1 身份标识符管理

负责与底层身份平台通信，身份标识符的生成、存储、销毁全生命周期管理。

个人及组织机构在身份平台注册时，平台会要求个人或组织机构进行实名认证，并为注册用户分配唯一的身份标识符。

#### 3.2.5.2 凭证发行方管理

组织机构完成注册后，可申请成为凭证发行方。凭证发行方可以发布凭证模板并为其他用户发行凭证以及凭证的验证。

### 3.2.5.3 凭证使用方管理

组织机构完成注册后，可申请成为凭证使用方。凭证使用方一般为第三方应用，根据业务需要通过身份平台到凭证发行方验证用户声明的属性（凭证），验证通过后根据设定的逻辑为用户提供服务。

### 3.2.5.4 凭证模板管理

组织机构认证成为凭证发行方后，可以发行凭证模板，表明本机构可以发行及验证的凭证类型、凭证内容等。

### 3.2.5.5 凭证管理

用户可以根据凭证发行方的凭证模板申请凭证，通过凭证发行方的认证后即可获得申请的凭证。并且可在业务需要时选择出示该凭证，第三方可通过身份平台到凭证发行机构验证所出示的凭证，以便继续为用户提供服务。

## 3.2.6 运维管理

### 3.2.6.1 通道浏览器

通道浏览器可以查看通道统计信息，包括活跃节点数、业务模型数量、智能合约数量、区块高度、交易总数、最近日交易量等信息。通过授权还可以在线查看区块链底层存储的数据信息，包括区块信息、交易信息、合约信息、账户信息等。

平台还支持根据区块编号、区块哈希、交易 ID 查询区块以及区块中的交易信息，点击交易 ID 还可以显示交易记录信息（交易 ID、交易时间、交易状态、执行的合约及其版本、写数据集等）。

### 3.2.6.2 快速自动化部署

用户准备好所需的主机资源（支持 Docker 及 Kubernetes (K8S) 类型的主机资源），输入区块链相关配置，即可快速、自动化部署区块链网络。

除了支持荣泽自主知识产权的区块链技术平台 RBC 2.4 的快速自动化部署与运维，同时还支持 Fabric 1.4、FISCO 2.x 等国内外主流区块链技术平台的自动化部署与运维。

### 3.2.6.3 监控与告警

可以监控区块链节点的 CPU、内存、上下行网络情况，并在节点故障时通过多种途径告警并通知运维人员，以便运维人员及时处理、消除故障。

支持实时监控与查看指定时间段的历史数据。

### 3.2.6.4 可视化看板

可视化看板分为区块链概览、通道浏览器。

区块链概览可以查看指定区块链网络的组织/联盟成员数量、通道数量、节点数量、账户数量、智能合约数量、业务模型数量等。

通道浏览器可以查看指定通道下的组织/联盟成员数量、活跃节点数量、区

块高度、智能合约数量、业务模型数量等。还可以根据区块号及交易 ID 查找区块信息及交易信息。

### 3.2.7 安全与隐私保护

RBaaS 提供多层多重安全防护与隐私保护。

#### 3.2.7.1 安全防护

传输层：所有通信（区块链节点间、RBaaS 与区块链节点间、区块链应用与 RBaaS 及区块链节点间、浏览器及 RBaaS 间）全部采用 SSL/TLS 安全传输通道，保障数据不会被泄漏、不被重放攻击。SSL/TLS 加密算法支持 ECC（椭圆曲线加密）及国密算法。

P2P 网络：联盟链的许可机制保证接入到区块链网络的节点都是通过认证的，防止非法节点接入及攻击。通过 CA 的公私钥（非对称加密/签名）机制实现节点的认证，加密/签名算法支持 ECC（椭圆曲线加密）及国密算法。

共识算法：可插拔的共识算法，保障数据的一致性并且不被恶意节点的破坏。

分布式账本：分布式全量账本，保障数据不被篡改、损坏及丢失。

拒绝服务：RBaaS 黑白名单机制，保障系统的安全。针对每个区块链网络设置的黑名单或白名单，将有威胁的地址排除在外。

#### 3.2.7.2 隐私保护

传输层：SSL/TLS 安全传输通道保障数据不会在传输中被泄漏。

数据存储：加密服务将保存到分布式账本中的数据加密，保障存储中的数据不被泄漏。

访问控制：提供模型库级、模型表级、字段级、行级访问控制，非授权账户无法访问隐私数据。

拒绝服务：针对每个区块链网络可以设置自己的黑白名单，只允许自家网络接入，进一步保障数据不被泄漏。

应用层：通过运行在安装沙箱中的智能合约实现业务逻辑，隐私数据不出区块链网络，实现数据的可用不可见，保护了数据使用中的隐私。

## 4. 产品应用领域

### 4.1 政务领域

政务信息化发展的难点在资源整合与应用，打破“各自为政、条块分割、烟囱林立、信息孤岛”的问题。由于业务烟囱的存在，其业务系统间不同数据格式、不同数据标准、不同数据管辖权造成了数据鸿沟，以及行政资源的浪费与行政效率的低下，无法实现政府内部纵向或横向协同，跨部门业务由业务申请人在数个政府部门之间奔跑传递。利用区块链技术更好的服务于政务，有助于打破信息孤岛、促进协同、降低成本提高效率、提升政府透明化治理等作用。

### 4.2 金融领域

区块链能够提供信任机制，具备改变金融基础架构的潜力，成为链上的数字资产，在区块链上进行存储、转移和交易。区块链技术的去中心化，能够降低交易成本，使金融交易更加便捷、直观和安全。区块链技术与金融业相结合，必然会创造出越来越多的业务模式、服务场景、业务流程和金融产品，从而给金融市场、金融机构、金融服务及金融业态发展带来更多影响。

#### 4.3 公共服务领域

传统的公共服务依赖于有限的维度，获得的信息可能不够全面且有一定的滞后性。区块链不可篡改的特性使链上的数字化证明可信度极高，在产权、公证及公益等领域都可以以此建立全新的认证机制，改善公共服务领域的管理水平。

#### 4.4 供应链领域

供应链是一个商流、物流、信息流、资金流所共同组成的，并将行业内的供应商、制造商、分销商（零售商、批发商）、终端用户串联在一起的复杂网链结构。而区块链技术作为一种大规模的协作工具，与生俱来地适用于供应链领域。例如：区块链+物流、区块链+溯源防伪等。

#### 4.5 物联网领域

物联网（IoT）蓬勃发展的今天，它不仅给个人消费带来变化，还给整个社会发展带来了深刻变化。目前，大型的物联网平台依靠中心化模型控制各个电子设备之间链接与交互，但是在很多场景下，这种方法变得不是那么实际。而分布式物联网平台正好可以解决这一问题。区块链技术可以帮助实现物联网平台的分布式数据存储，交互，保证数据的安全性和可信性，同时可以记录数据交互的信息。区块链在工业设备、智慧交通与智慧城市等领域都可以有很好的应用。

#### 4.6 医疗领域

医院是医疗数据的关键卡位，电子病历是医疗信息化的核心数据。传统的中心化信息管理系统的模式，仍然存在区域限制问题、信任问题、服务稳定性问题以及全面信息归集等问题。区块链有助于加快健全完善医疗救助服务，为困难群众提供高效、便捷的事后救助结报，通过具有资质的商业保险机构参与医疗机构合作，让更多的人可以先看病后还款。利用区块链技术进行药物防伪就是商品溯源的一个具体行业应用。药品溯源可以追踪记录药品从生产到零售的全部环节，药品溯源属于一种多环节协同的综合性商业行为，集合了 IOT 技术、防伪技术、信息系统与溯源机制。

#### 4.7 数字版权领域

版权领域的痛点还在于维权门槛高，传统数字内容的版权维护路径，需要内容生产者向监管部门提出版权认证申请，需要耗费较多的时间与金钱。但处于区块链的环境下，内容生产者或机构都可以通过加入区块链网络社区，方面快捷的实现内容上链，版权登记。版权内容生产者将自己的作品传到区块链平台上，平

台为作品生成一个不可篡改、准确原创证明的唯一 ID，证明版权的归属和完整性，并同时记录到链上，维权成本和门槛极低。

在维权门槛较低的同时，区块链数字版权的法律效力也能得到保障。相比传统的维权取证来源，监管部门更看重维权取证的证明力，而区块链的数字维权证明有别于人为的信用委托，更趋向与数据代码构成的技术背书，同时公信力更有效。

通过区块链技术，还可以对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。作品在区块链上被确权后，后续交易都会进行实时记录，实现数字版权全生命周期管理，也可作为司法取证中的技术性保障。

#### 4.8 公益领域

在公益事业蓬勃发展的过程当中，其透明度和公民信任度也愈加模糊，这也是诸多人士关注的一个大问题，捐赠金额的去向不明不白，也是公益圈一个值得重视并解决的问题。

区块链上存储的数据，高可靠且不可篡改，天然适合用在社会公益场景。公益流程中的相关信息，如捐赠项目、募集明细、资金流向、受助人反馈等，均可以存放于区块链上，并且有条件地进行透明公开公示，方便社会监督。

#### 4.9 数据服务与共享

数据作为数字经济的生产资料，只有流通起来才能产生社会价值与经济价值。目前数据的流通面临隐私泄漏与信息保护等多种问题。利用区块链可追溯、不可篡改的特性，可以确保数据来源的真实性，同时保证数据的不可伪造性，区块链技术将从根本上改变信息传播路径的安全问题。同时利用智能合约，数据可用不可见，进一步保护用户隐私以及数据生态的利益。