区块链服务

产品介绍

文档版本 01

发布日期 2023-08-14

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

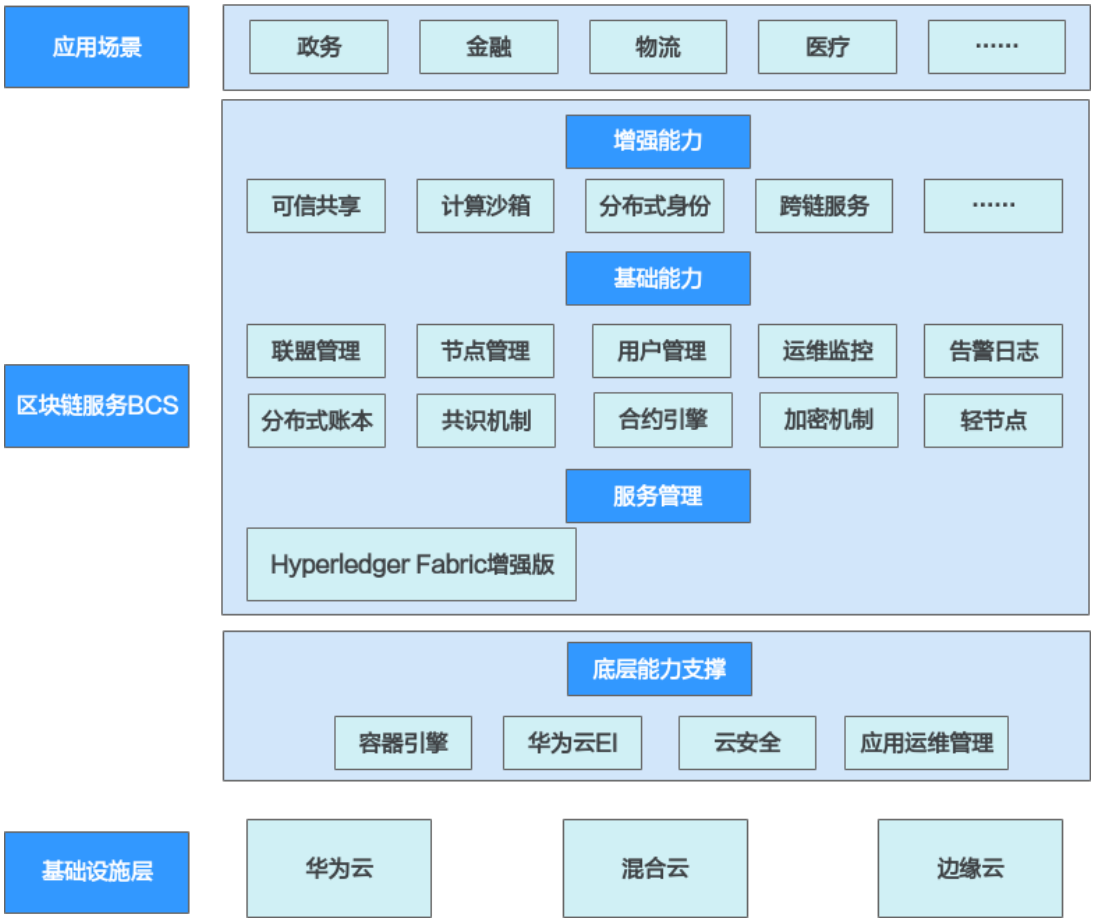
目 录

1 图解区块链服务

2 什么是区块链服务

区块链服务（Blockchain Service简称BCS）是面向企业及开发者提供的区块链技术服务平台，它可以帮助您快速部署、管理、维护区块链网络，降低您使用区块链的门槛，让您专注于自身业务的开发与创新，实现业务快速上链。

图 2-1 产品架构



- **基础设施层**

  创建区块链网络需要使用的底层资源，包括节点计算资源、存储资源等，用于网络中数据计算及存储。

- **区块链服务BCS**

  区块链服务BCS，支持创建Hyperledger Fabric增强版实例，包括用户管理、节点管理、运维监控等模块，帮助您快速创建、方便管理、高效运维区块链网络，为上层应用提供企业级区块链系统。

  - Hyperledger Fabric增强版：以Hyperledger Fabric 为内核，基于全栈可信能力，包括弹性服务器，企业级容器、安全和人工智能等服务，在保持无缝社区对接方式前提下，在可靠性、性能、隐私保护方面做了增强和提升，满足企业级和金融级业务要求。

- **应用场景**

  区块链服务BCS可应用于各大行业的多种场景中，各行业的业务应用对接区块链平台，保证业务数据可信、安全。

- **安全管理**

  基于轻节点的隐私隔离、共识算法、国密加密算法等。提供安全计算、可信数据共享、分布式身份等能力。

区块链的价值

经济高效：构建可信多方协作平台，减少人为纠纷，提高交易效率。

降低成本：减少额外开销和中间第三方的参与。

减少风险：不可篡改性降低了欺诈和网络错误的发生。

增进信任：共享的账本、流程、记录增进参与方之间的可信度。

透明审计：审计机构可随时对不可篡改的账本进行审计。

知识扩展

- 区块链系统中的数据以区块（block）为单位产生和存储，并按照时间顺序连成链式（chain）数据结构，故名区块链。
- 所有节点共同参与区块链系统中的数据验证、存储和维护。新区块的创建需要得到共识确认，并向各节点广播实现全网同步，同步之后不能更改或删除。

3 产品功能

区块链服务为您提供如下功能，助您快速，安全、高效、低成本上链。

区块链实例部署

您无需提前准备区块链系统需要的资源，可一键式完成购买资源与部署区块链网络。

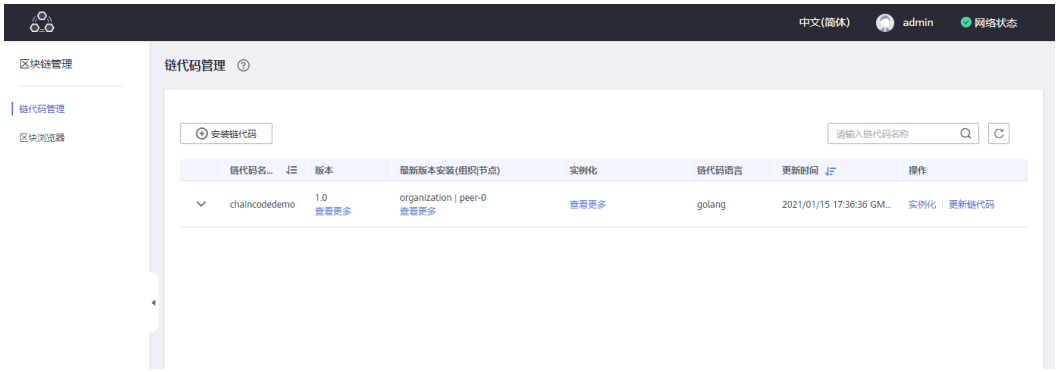
- 部署时间从天级降至分钟级，一步到位完成区块链网络的配置和部署。
- 屏蔽底层技术细节，无需关注区块链底层技术实现和平台构建。
- 支持创建联盟链和私有链的区块链类型。

实例管理

提供区块链实例管理功能，可实时查看区块链实例运行状况，并对区块链实例做相应的操作，例如添加组织、更新版本、获取客户端配置等。

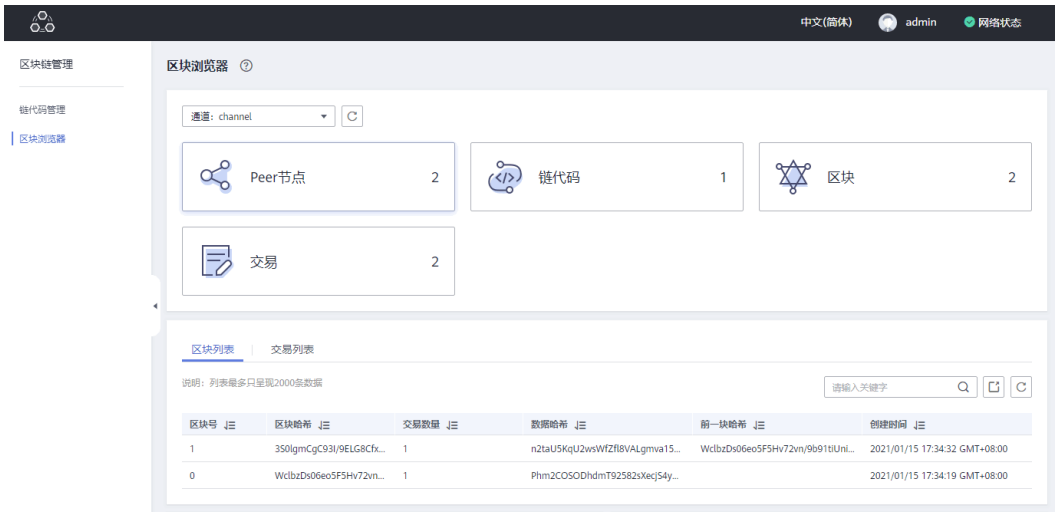
链代码管理

通过图形化界面可视化管理链代码的全生命周期：链代码编码、调试，安装链代码、实例化链代码和更新链代码。



区块浏览器

区块链浏览器提供区块链相关信息的查询，包括区块数量、交易数量、区块详细信息、性能数据及节点状态、区块列表、交易列表及交易详情信息等，帮助您了解整个区块链的状态，对区块链基本的维护提供数据支撑。



账本存储

提供文件数据库（GoLevelDB）和NoSQL（CouchDB）两种区块链状态信息存储可选方案。

- 文件数据库：交易历史数据保存在区块链中，状态数据保存在LevelDB中。
- NoSQL：CouchDB存储交易数据和状态数据。

共识算法

提供两种算法以适应不同场景。

- Raft(CFT)：可保证部分排序节点出现非拜占庭故障时系统的正确运行，在排序过程中最多可容忍 (N-1)/2 个故障节点存在（N为排序节点总数）。支持v2.2的Fabric内核。
- 快速拜占庭容错共识算法(FBFT)：需要4-10个排序节点。在排序过程中最多可容忍 (N-1)/3 个错误节点存在（N为排序节点总数）。支持v2.2的Fabric内核。

联盟成员/组织管理

- 联盟发起方可动态邀请其他成员加入联盟，快速组建区块链联盟链，既方便又灵活。各成员节点运行在独立的VPC中，独立管理，安全可控。
- 区块链实例同时支持动态添加节点组织，操作方便。

节点弹性扩容

根据用户需求，无需重启系统，支持节点弹性扩容。

合约扫描

通过自动化分析工具，为智能合约应用商和开发者提供代码安全审计，借助广泛的联盟链合约漏洞检测内容和问题检测库，生成检查报告及时发现代码中的安全隐患并提供修复建议，力求从源头上确保智能合约安全。

隐私保护

- 同一个通道内可以通过隐私保护配置确保不同成员数据的隐私性。

  例如A、B成员，经过隐私保护配置，指定A成员可以访问相关数据的权限，只有拥有指定权限的成员A能访问相关数据，没有权限的成员B，则无法访问相关的数据，保证在一个共享通道内数据的隐私性。
- 不同通道之间通过通道隔离实现数据隐私保护，可以理解为通道外的成员无法获取该通道内的区块信息。

应用接入

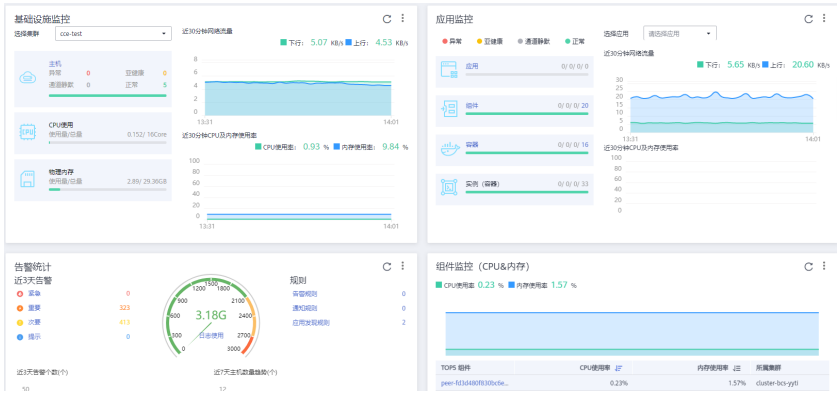
提供应用接入方式为：SDK和RESTful接口。

- 提供SDK配置文件下载功能，简单配置即可完成应用与区块链网络的对接。
- 提供RESTful接口调用链代码功能，应用可以通过RESTful接口直接调用链代码。同时支持多组织背书。

监控运维

对接监控服务平台对数据和资源实时监控、告警、通知。

- 自动化运维：主动升级底层区块链平台和更新补丁，与华为云运维系统无缝集成。
- 企业级监控：集群全天候实时多维度监控，同时可自定义并上报多渠道告警。



4 产品优势

开放易用

自建企业级分布式区块链网络并非易事，不仅需要深入专业的区块链知识，同时需要各种复杂的设计和配置，易出错，投入成本高。

- BCS可以帮助企业最快5分钟内完成区块链网络部署，可节省80%的开发和部署成本。
- 提供全生命周期管理和界面化的智能合约编码、调试与部署。让用户简单使用区块链系统，专注于自身业务应用的创新与开发。

灵活高效

- 支持多种高效共识算法，深度优化已有算法，在安全和效率上达到平衡点。
- 秒级共识（100000TPS+），满足业务性能需求。
- 区块链账本存储在华为云高效弹性存储文件中，满足用户海量快速存储需求。
- 支持多角色节点和成员动态加入/退出，支撑用户高效组建联盟链。

高性价比

- 按需付费、随时休眠/唤醒，减少使用成本。
- 对接运维平台AOM对区块链服务进行统一运维，为客户提供全系列的系统状态、性能和交易情况的监控，运维，报警能力，能为用户降低运维成本。
- 提供节点伸缩功能，用户可根据需求进行弹性伸缩，大大提高使用性价比。

安全隐私保障

全方位保护区块链安全：

- 华为云自身安全体系保护区块链稳定运行。
- 基于Hyperledger的安全体系通过证书管理、链式数据结构等手段实现不可篡改、隐私保护。
- 自主创新的同态加密、零知识证明等算法提供更进一步的安全隐私保护。
- 支持基于国密算法的加解密。

可信协作

基于区块链构建多方可信协作的基础设施：

- 基于W3C的DID标准和VC（DID可验证声明）标准，支持分布式身份管理能力，降低合作各方间信任成本、提升整体协作效率。
- 基于区块链构建数据可信共享平台，促进多方数据可信流动、打破数据孤岛，发挥数据价值。
- 基于区块链、TEE（Trusted Execution Environment）技术和联邦学习等技术构建数据不出域的安全计算能力，达到数据可用不可得，充分保障用户数据隐私。

5 基本概念

区块链

根据工信部指导发布的《区块链技术和应用发展白皮书》的解释：狭义的讲，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和存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全性、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

分布式账本

分布式账本是一种在网络成员之间共享、复制和同步的数据库。分布式账本记录网络参与者之间的交易，比如资产或数据的交换。这种共享账本消除了调解不同账本的时间和开支。手册中提到的账本均指的是分布式账本。

- 去中心去信任：多份数据分布保存在各个节点，没有中心化或第三机构负责控制数据。
- 集体维护数据一致：参与者以公钥作为身份标识，各节点独立校验数据合法性，各节点共识决定写入哪些数据。
- 数据可靠难以篡改：数据在区块中，各节点保存全部区块。可定制数据访问权限，块间的链式关联防止篡改数据。

智能合约

即链代码，是运行在区块链上的、特定条件下自动执行的代码逻辑，是用户利用区块链实现业务逻辑的重要途径。基于区块链特点，智能合约的运行结果是可信的，其结果是无法被伪造和篡改的。

- 过程无法作弊：满足条件自动触发，执行结果独立验证。
- 结果不能修改：数据保存在区块链。
- 合约内容可靠：智能合约内容保存在区块链中。
- 隐私保护：只有指定的参与方可以获取合约内容、数据。

peer 节点

维护账本的网络节点，一个或多个peer节点组成peer组织。

共识节点

区块链网络中参与交易的节点。

通道

通道可以将区块链网络中的账本数据进行隔离和保密，主要用于实现联盟链中业务的隔离，每个通道可视为一条子链，并且对应一套账本，同一个区块链网络，不同通道之间的账本数据不可见。

分布式共识

系统中多数独立参与者对某个交易/操作的有效性达成一致。包括对双方交易的验证达成一致、对任何交易的其他合法性（比如业务逻辑合法性）的验证达成一致、对于合法数据是否写入现有账本达成一致。

哈希算法

一段数字内容的Hash值，可以用于验证数据的完整性。数字内容的微小修改都会引起Hash值的巨大变化。合格的Hash算法很容易由数字得到Hash值，却几乎不可能通过Hash值反算出原数字内容。

组织

在通道中一般包含有若干成员（组织），若两个区块链网络实体的身份证书能够追溯到同一个根CA，则认为这两个实体属于同一组织。

6 产品规格差异

Hyperledger Fabric 增强版

区块链服务BCS提供基础版、专业版供您选择使用，每个版本均有不同的规格支持，详细请参见表6-1。集群规格信息请参考表6-2。

各版本的价格请参见：产品价格详情。

说明

一个容器集群目前只能部署一个区块链实例。

表 6-1 各版本区别

功能		基础版	专业版
适用场景类型		满足小规模商用	满足中等规模商用
联盟链		支持	支持
交易峰值性能		不超过500 TPS	不超过2000 TPS
共识算法	Raft(CFT)	支持	支持
	FBFT	不支持	支持
节点管理	最大成员组织数	2	5
	单组织最大成员节点数	2	2
	最大共识（Orderer）节点数	3	4
	最大通道数	2	4
	节点故障自动恢复	支持	支持
	节点弹性伸缩	支持	支持
	最大轻节点数	不支持	10
安全功能	ECDSA	支持	支持

功能		基础版	专业版
	国密	不支持	支持
	加法同态	不支持	支持
	零知识证明	不支持	支持
高可用	Restful接口调用智能合约	支持	支持
	普通部署	支持	支持
	高可用部署	不支持	不支持
运维监控	运维日志	支持	支持
	节点状态监控	支持	支持
	状态告警	支持	支持
服务支持	专属服务经理	不支持	不支持
	研发远程技术支持	不支持	不支持
	点对点故障处理客户现场支持	不支持	不支持

表 6-2 规格信息

规格	CCE规格	ECS节点	EIP	VPC及subnet	容器网络
基础版	cce.s1.small （小规模单控制节点CCE集群，最大50节点） 单AZ	规格：4核8GB 个数：组织节点(peer)数/2+1个(orderer)	私有链：不创EIP 联盟链：每个集群节点(node)1个eip EIP带宽大小：1M	1个VPC及subnet	VPC网络
专业版	cce.s2.small （小规模高可用CCE集群，最大50节点） 多AZ	规格：8核16GB 个数：组织节点(peer)数/2+orderer数	私有链：不创EIP 联盟链：每个集群节点(node)1个eip EIP带宽大小：5M	1个VPC及subnet	VPC网络

7 应用场景

7.1 公司间交易

区块链服务为公司间交易构建由跨国集团各辖区各子公司和审计机构作为参与方组成的协作联盟，帮助双方提高信任，消灭对账及差异，提供全程审计支持。

行业现状及痛点

- **公司间信任问题**

  交易双方由于并非完全信任，在合同约定执行、交易过程中物权转移、资金转移存在信任问题。
- **延迟财务结算**

  由于内部交易对账需要耗用大量的人力和时间，对账的差异很可能引起账务结账的延迟，报表出具延迟。
- **效率低下和高成本**

  内部对账过程冗长，需大量财务人员工作和时间，而且对账结果并不理想，监管更不容易。
- **数据无法共享**

  集团下各公司间财务数据分布于不同类型的ERP中，不同系统间没有集成，各系统间不互通。
- **与监管方之间缺乏信任**

  跨国集团公司必须保留多年的记录（通常为10年或更长时间），并向外部审计师/当局证明数据来源和未被篡改。
- **重复问题**

  公司间转移定价及复杂的交易业务问题可能造成税基侵蚀和利润转移（BEPS），存在报表重述的风险。

方案架构

基于区块链服务可以实现：

- **统一化账本**

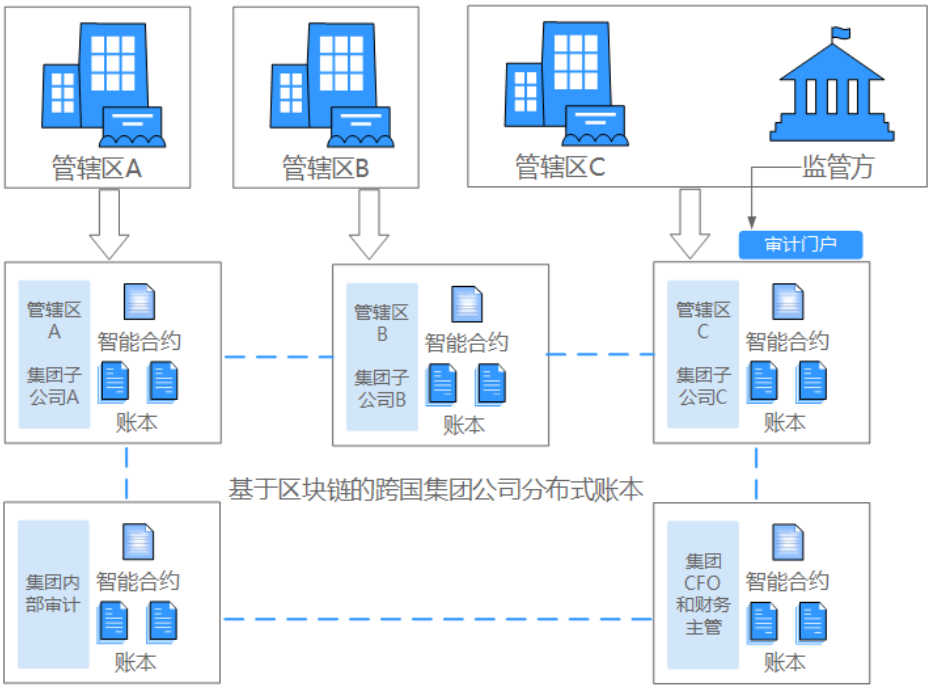
  提供不可篡改、可追溯的一致性业务交易记录，消除双方对账工作，满足审计追溯。

- **数字资产化**

  对交易资产和权益的Token化，实现数字资产的生命周期管理。
- **履行智能合约**

  实现自动化处理，保证了按照条款忠实执行的公正性。

图 7-1 方案架构



方案优势

- 消灭了公司间对账工作，保证公司间交易一致性和账务平衡性。
- 利用Token跟进货物的状态、时间、物理位置和所有权变更，将合同条款完全融入交易过程，提升双方信任。
- 精简和规范公司间供应链流程。
- 支持了不同系统之间的公司间事务处理。
- 为内部审计和外部审计提供端到端可追溯和不可篡改的信息。

7.2 供应链物流

基于区块链服务，同时结合物联网技术，构建由生产商、仓储、物流商和客户作为参与方组成的协作联盟，将货物从生产，仓储、干线物流，经销商，本地物流一直到客户全流程信息的可信记录，解决了信息孤岛，信息流转不畅，信息缺乏透明度等行业问题。

行业现状及痛点

- **纸质单据**

  很多环节仍然大量沿用手工操作和纸质单据，导致运单流转时间长、成本高、对账慢、易丢失和污损，文件成本占物流成本的1/5。

- **效率低**

  供应链各协作方信息系统独立，没有统一的标准和信息系统，协作方之间协作和作用难度大。

- **周期长**

  电子信息易被篡改，只能采用纸质单据作为结算的唯一凭据，上下游核算周期长，承运商的平均应收款账期较长。

- **融资难**

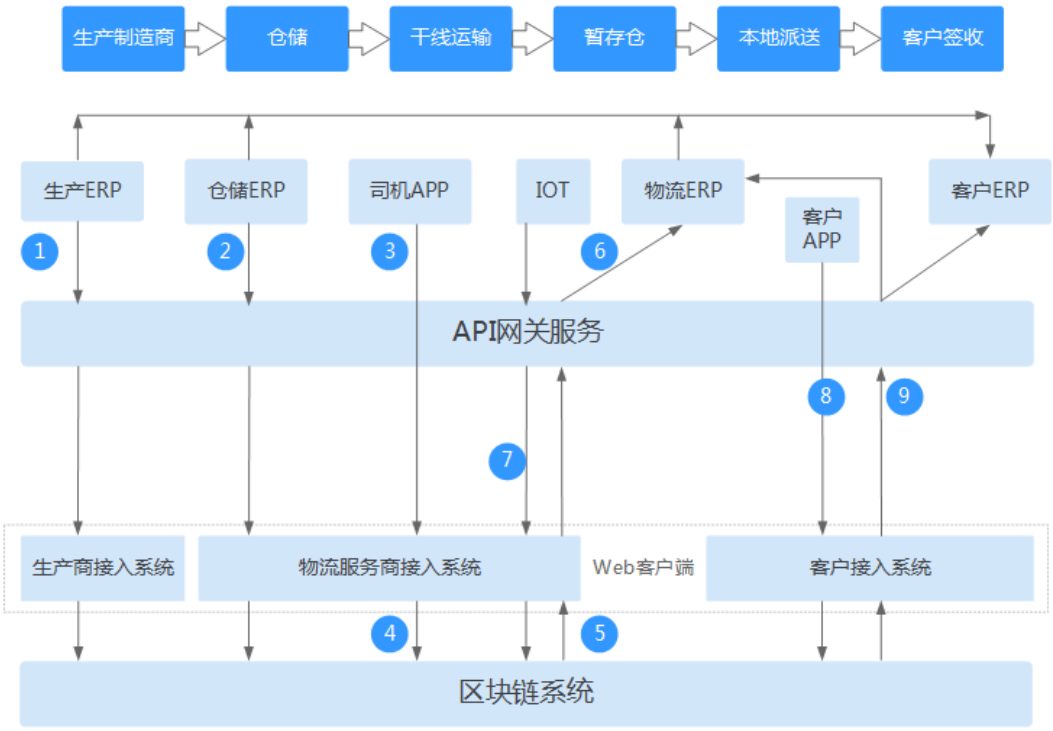
  承运商大多为中小企业，缺乏信用记录，信用积累和数据，融资难，融资成本高。

方案架构

区块链供应链物流与现有参与方IT信息系统的结合，可实现：

- 统一化账本。提供不可篡改、可追溯的一致性货物流转记录，满足审计要求。
- 为参与方IT系统提供通用接口接入区块链服务，相关信息输入不可篡改，各自为自己的信用买单，逐步建立信任体系。
- 通过司机APP附加地址围栏信息自动输入实现实时展示“由谁，在什么时间，在什么地方”处理货物。
- 履行智能合约。实现自动签收和结算，自动运算输出绩效结果，公平公正。

图 7-2 方案架构



流程描述：
1、发货信息由接入系统上传区块链。
2、收发货信息经接入系统上传区块链。
3、司机扫描货物信息。
4、物流信息经接入系统上传区块链。
5、区块链回复确认信息已写入。
6、信息通过API网关写入IT系统。
7、卡车GPS信息经服务器上传区块链。
8、客户收货信息经服务器上传区块链。
9、区块链确认信息已写入并上传写入LSP和生产商ERP。

方案优势

- **减少错误**

  分布式共享账本极大改善供应链的可追溯和透明度，可有效减少或消除欺诈和错误。
- **提高效率**

  通过电子POD，减少纸上作业造成的延误，通过智能合约自动结算，提高效率。
- **降低成本**

  通过快速结算，自动接单，有效跟进，可以有效降低各方的物流成本。
- **透明审计**

  不可篡改的分布式账本，不可抵赖的签名，能快速有效的发现供应链物流中存在的问题。
- **提高信任**

  货物从生产、运输到最终接收，通过区块链技术可以实现全程跟进，规则透明，自动结算，可以极大提高消费者和第三方的信任。

7.3 医疗健康

区块链服务为医疗健康构建由各医疗机构、第三方机构和监管部门作为参与方组成的协作联盟，通过不可篡改、隐私保护的电子病历打通医疗信息孤岛，帮助医患双方提高信任，让患者拥有全面的健康和医疗信息，为远程医疗和转诊医疗提供基础。

行业现状及痛点

- **数据不安全**

  医疗健康数据大多存储在数据中心，如果数据中心发生自然灾害、黑客入侵等，那么患者的电子病历就有可能会彻底丢失。

- **信息孤岛**

  医疗机构之间没有合理的互信机制和良好的分享机制，容易形成“信息孤岛”，不利于数据的完整性和全面性。信息的可靠性以及在共享中信息的随意修改都成为面临的主要问题。

- **重复医疗**

  由于各个医院和机构之间信息不互通，患者去一家医院就会在该医院建立一份电子病历，使患者重复做各种检查，耽误时间、金钱以及医疗资源。

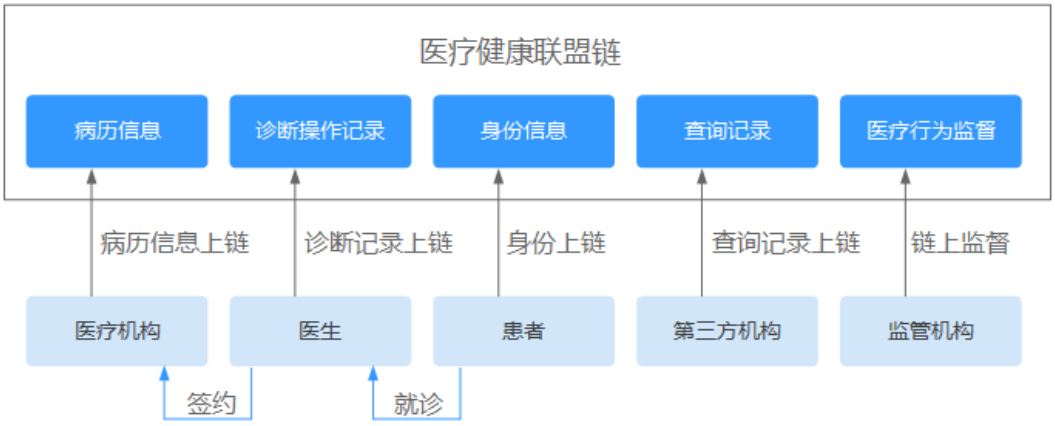
- **无获得感**

  医疗资料存放在医院系统中，患者对自己的数据不了解，也无法掌控，患者的就诊与健康管理受有限资料的限制。

方案架构

通过由医疗机构、第三方机构、医生、患者和监管机构组成的基于电子病历的医疗健康联盟链，将医疗和健康数据上链，通过加密技术和智能合约授权机制，实现患者数据安全授权查询，支撑科研数据确权隐私使用。实现安全、共信和确权。

图 7-3 方案架构



方案优势

- **打通信息孤岛**

  通过医疗联盟链，打通整个医疗机构信息系统，将区域检验、超声和放射结果互通互认，实现网络门诊、双向转诊和远程会诊。

- **不可篡改**

  通过将电子病历，医生诊断过程和结果、病历查询记录和病人身份上链，确保信息不可篡改，访问可跟进，减少医患纠纷，构建和谐医疗环境。

- **保护隐私和知情权**

  通过加密和合约授权机制，严格保护患者医疗隐私信息，做到患者全掌握，他人使用需授权。

- **快速有效监管**

  所有数据上链，监管机构在用户授权下可以快速有效监管医疗行为，有效防止违规行为和医患纠纷。

8 权限管理

如果您需要对华为云上购买的BCS资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云帐号中给员工创建IAM用户，并使用策略来控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望员工拥有BCS的使用权限，但是不希望员工拥有删除BCS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用BCS，但是不允许删除BCS的权限策略，控制员工对BCS资源的使用范围。权限管理的详细介绍及其权限配置操作，Hyperledger Fabric增强版请参考**权限管理**。

如果华为云帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用BCS服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。

权限根据授权精细程度分为角色和策略：

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

Hyperledger Fabric 增强版权限

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

BCS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问BCS时，需要先切换至授权区域。

如表8-1所示，包括了Hyperledger Fabric增强版的所有系统权限。

表 8-1 Hyperledger Fabric 增强版系统权限

系统权限	权限描述	权限类别	依赖关系
BCS Administrator	区块链服务Hyperledger Fabric增强版的所有执行权限。	系统角色	Tenant Guest、Server Administrator、ELB Administrator、SFS Administrator、SWR Admin、APM FullAccess、AOM FullAccess、CCE Administrator、VPC Administrator、EVS Administrator、CCE Cluster Admin
BCS Fabric FullAccess	区块链服务Hyperledger Fabric增强版的所有权限。	系统策略	无
BCS Fabric ReadOnlyAccess	区块链服务Hyperledger Fabric增强版只读权限。	系统策略	无

- BCS Fabric FullAccess策略内容：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "bcs:fabric*:*",
                "cce:*:*",
                "ecs:*:*",
                "evs:*:*",
                "vpc:*:*",
                "elb:*:*",
                "aom:*:*",
                "apm:*:*",
                "rds:*:*",
                "dms:*:*",
                "sfs:*:*",
                "sfsturbo:*:*",
                "cloudIDE:*:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

- BCS Fabric ReadOnlyAccess策略内容：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "bcs:fabric*:get*",
                "bcs:fabric*:list*",
```

```
            "cce:*:get*",
            "cce:*:list*",
            "ecs:*:get*",
            "ecs:*:list*",
            "evs:*:get*",
            "evs:*:list*",
            "vpc:*:get*",
            "vpc:*:list*",
            "elb:*:get*",
            "elb:*:list*",
            "aom:*:get*",
            "aom:*:list*",
            "apm:*:get*",
            "apm:*:list*",
            "rds:*:get*",
            "rds:*:list*",
            "dms:*:get*",
            "dms:*:list*",
            "sfs:*:get*",
            "sfsturbo:*:get*",
            "cloudIDE:*:get*",
            "cloudIDE:*:list*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

9 计费说明

Hyperledger Fabric增强版不同版本实例管理费收费标准请查看**价格详情**。

10 约束与限制

区块链服务对配额进行了限制，最多支持创建5个Hyperledger Fabric增强版实例。每个实例按照版本不同支持不同的规格，详细信息参见**产品规格差异**页面。

11 停止维护版本

版本小于2.1.33已不再维护，如果您使用的BCS版本小于2.1.33，部分操作可能受限，请您尽快升级至最新版本。

12 安全公告

12.1 Apache Log4j2 远程代码执行漏洞（CVE-2021-44228）公告

漏洞描述

近日，关于Apache Log4j2存在一处远程代码执行漏洞（CVE-2021-44228），在引入Apache Log4j2处理日志时，会对用户输入的内容进行一些特殊的处理，攻击者可以构造特殊的请求，触发远程代码执行。目前POC已公开，风险较高。具体漏洞详情，请参见**Apache Log4j2 远程代码执行漏洞（CVE-2021-44228）**。

漏洞影响

在区块链服务（简称BCS）中提供的国密加密Fabric_SDK_Gateway_Java和Fabric_SDK_Java、开源社区的Fabric_SDK_Gateway_Java和Fabric_SDK_Java及BCS提供的对应示例Demo App_Gateway_Java_Demo、App_Java_Src_Demo、App_Java_Jar_Demo中有使用Apache Log4j2。

当前BCS已在华北-北京四Region修复以上组件的漏洞，如您使用了以上组件，请尽快至华北-北京四Region的应用案例获取最新版本并完成升级以避免安全风险。在完成漏洞修复前，请确认您区块链应用的输入源是否可信。

漏洞规避方案

升级您区块链应用中的Fabric_SDK_Gateway_Java、Fabric_SDK_Java及Apache Log4j2至最新版本。

已修复漏洞的Fabric_SDK_Gateway_Java和Fabric_SDK_Java可在华北-北京四Region的应用案例中获取，使用方式可参考：**国密加密->SDK使用->安装SDK**。