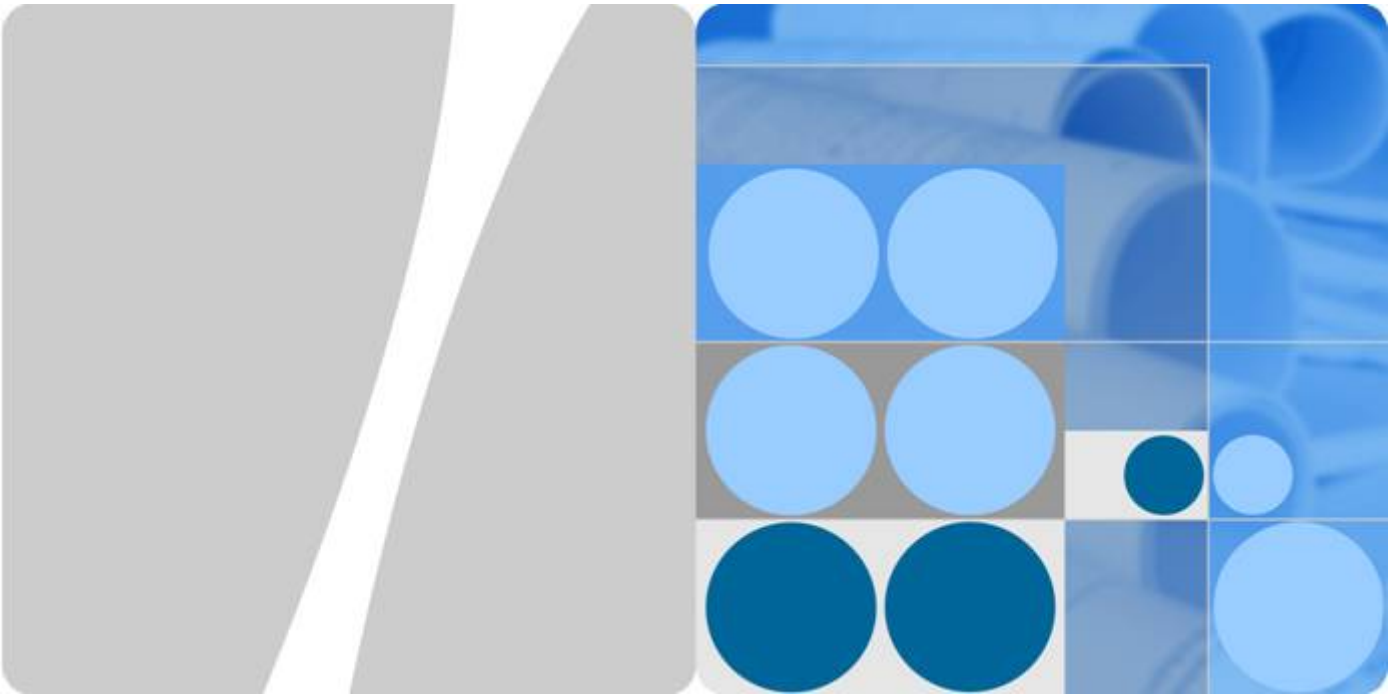


区块链服务

产品介绍

文档版本　01

发布日期　2018-03-30

华为技术有限公司

HUAWEI

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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 产品概述

区块链服务 BCS

华为云区块链服务（Blockchain Service）是面向企业及开发者的高性能、高可用、高安全区块链技术平台服务，可以帮助客户在华为云上快速、低成本的创建、部署和管理区块链应用及商业智能合约服务。

2 产品功能

区块链服务为您提供六大功能，助您快速上链，安全、高效、透明。

一键式快速部署

相对于自建区块链部署时间从天级降低到分钟级。

- 低门槛、高效率的区块链使用

  部署时间从天级降至分钟级，完全自动化生成配置，内置最佳实践，可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

  无需担心区块链底层技术实现和平台构建，即买即用，平台提供高可用、高性能和高安全的区块链系统，用户只需专注业务创新。

成员动态加入

邀请华为云租户，快速组建区块链联盟，各成员节点运行在独立的VPC，独立管理，安全可控。

由发起方邀请联盟链其他成员加入，既方便又灵活，区块链网络的成本由其成员分摊。

共识算法可插拔

提供多种算法以适应不同场景。

- 简单测试共识算法SOLO

  简单共识算法，只需启动一个节点即可提供共识排序功能，不支持拜占庭容错，启动快速，节约资源，推荐测试时使用。
- 快速拜占庭容错共识算法FBFT

  高性能、高可用容错共识算法，需要至少4个节点才能提供交易共识排序功能，可容忍不大于（N-1）/3个拜占庭错误节点，建议生产环境使用。
- Kafka(CFT)算法

节点弹性伸缩

根据用户高可用要求，无需重启系统，支持peer节点弹性伸缩。

- 高可用

  集成Kubernetes，支持Master节点、共享存储、节点故障恢复。
- 动态扩展

  节点使用Docker容器运行，可以根据用户的需求，无缝进行扩展且不中断业务。

可视化链代码管理

通过界面方便管理链代码的全生命周期：链代码查看，链代码安装和链代码实例化。

云端监控

主动升级底层平台，提供开放性的云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。

3 产品优势

开放易用

基于Hyperledger、K8S和docker搭建；简单配置数分钟内完成区块链部署；自动化、全流程运维服务；集群全天候、实时多维度监控。

灵活高效

支持多种高效共识算法灵活切换；秒级共识（2000TPS- 10KTPS）；多角色节点和成员动态加入/退出；容器化物理资源管理。

高性价比

一键上链节约系统80%开发、部署成本；按需付费，减小60% 以上研发和初始成本；统一运维，节约监控和运维成本；可根据用户需求进行弹性伸缩。

安全隐私

完善的用户、秘钥、权限管理和隔离处理；多层加密保障和国密支持；同态加密等隐私处理；可靠的网络安全基础能力，运营安全无忧。

4 应用场景

供应链金融

挑战：

- 零部件多，供应商多，供应链层级多。
- 供应商的金融信用差异大。
- 零部件供应商的平均收款账期长。
- 间接供货的小供货商融资难，融资贵。

解决方案：

所有的供应商全部放入区块链，每一次发票挂账信息都会登记在这条链上。

价值：

- 主机厂除生产制造业务，通过金融机构赚到了金融服务的收益。同时更好的了解整个供应商网络。
- 供应商收款的平均账期更短，通过正规金融机构，融资成本更低更透明。
- 金融机构在风险可控的情况下，从“长尾客户”获得收益。通过资产证券化主机厂获得收益。了解供应链的真实贸易，利于开展其他金融服务。

供应链溯源

客户希望知道购买商品的供应链信息，比如车主希望知道每个零件是否是原厂生产，是否正牌渠道供货，比如消费者希望知道食品的生产、经销、运输过程。

挑战：

- 商品供应链权属关系（原厂、总代、分销、零售）和上下游关系（生产、总装、维修、保养）都比较长，每个企业各管一段。
- 商品形态出现很大的变化（例如小麦、面粉、饼干）。

解决方案：

区块链可以解决每一件商品的出处（例如一箱饼干来自哪一批面粉）。

价值：

- 把分段的输入输出关系串接起来。

- 全局一本账，杜绝凭空生出和凭空消失的零件。
- 对原厂渠道管理和政府市场监管有帮助。

证券交易

价值

- 区块链作为共享账本，在资产管理、托管 业务、审计之间共享托管业务的核心业务数据。
- 共享账本实现数据共享，更加准确判断报价的合理性。
- 托管人购买资产后的资产保存在区块链中，委托人可以随时查看存量资产情况，审计方也可以实时审计。
- 区块链智能合约自动判断交易的合理性和合规性。
- 通过基于区块链的系统来发送投资指令，代替原来的传真、电话方式。
- 不可篡改解决传统手段核对预留签印的问题，提高指令发送的执行效率。

其他场景

区块链可应用于众多行业及场景，还有食品安全、众筹公证、数字资产、国际贸易、私人记录、公共记录等等。

5 基本概念

区块链

狭义：一种保存记录（数据）的范式。

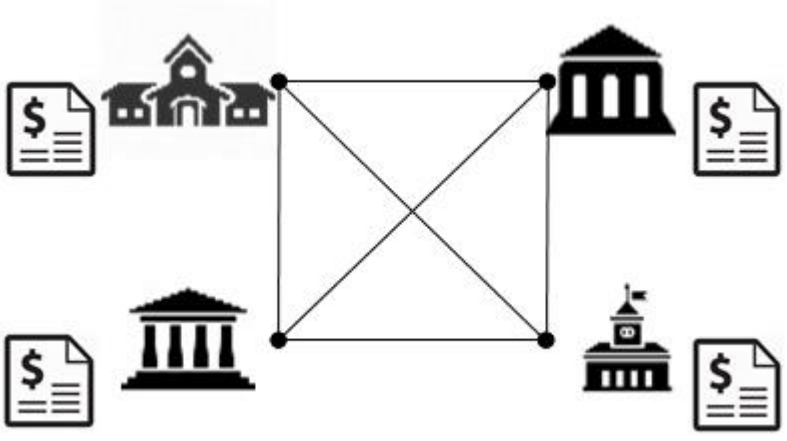
广义：基于可靠数据，通过智能合约执行去中心化可信计算任务。

所有数据保存在区块中，新写入的数据组成新的区块，添加在当前区块链末端。每个区块在保存数据的同时，还要保存前一个区块中所有记录的数据唯一对应的一个数（往往是所有数据的Hash）。

更多描述信息可在互联网上进行搜索查看、学习。

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。



- 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

维护账本的网络节点。

组织

联盟链中按照访问和使用账本的网络节点，一个联盟（或者一个区块链网络）有多个组织（成员），一个组织内可以有多个节点（ Peer ）。

通道

通道是为了实现数据的隔离和保密而构建在区块链网络上的私有区块链。每一个通道即为一条逻辑上的区块链。加入某个通道的Peer对该通道中的交易是可见的，同一个节点可以加入多个通道。

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。包括对双花交易的验证达成一致，对任何交易其它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。

公私钥体系

公私钥体系是现在加密通讯的基石，通过加密算法随机生成公私钥对，一般私钥需要在用户手中绝对安全保存，保证只有用户才能接触到，公钥可以对外公开。可靠的加密算法可以保证任何人无法通过公钥计算出其对应的私钥。

基于 PKI 的加密

加密一般是指向特定用户发送加密内容，保证只有接收方才能解密原内容。具体地，发送方用接收方的公钥加密原内容，得到密文，将密文发送给接收方，接收方用自己的私钥便可由密文解密（Decryption）出原内容。

基于 PKI 的签名

签名用于他人验证消息内容确实来自声明的内容发送者。具体地，内容发送者发送一段明文，并将明文的Hash用自己的私钥加密，生成签名。任何接收方收到明文后，同

样对明文进行Hash，然后用发送者的公钥解密签名，将得到的数据与自己对明文Hash的结果对比如果一致，则可以证明消息确实是该公钥对应的私钥持有者发出的。

6 使用限制

使用华为云区块链服务需要先购买云容器服务（CCE）并创建CCE集群，购买文件存储服务（SFS），再部署使用区块链服务及建立区块链应用。

7 版本说明

表 7-1 版本说明列表

发行时间	更新说明
2018-03-30	公测版本