
HUAWEI
华为区块链白皮书
构建可信社会，推进行业数字化
2018年4月

前 言

区块链成为近两年热点话题，因其通过分布式数据存储、点对点传输、共识机制、加密算法等技术的集成，可有效解决传统交易模式中数据在系统内流转过程中的造假行为，从而构建可信交易环境，打造可信社会。近年来各国政府机构，国际货币基金组织以及标准、开源组织和产业联盟等在纷纷投入区块链产业的拉通和应用。随着区块链的产业价值的逐渐确定，区块链迅速地成为一场全球参与竞逐的“军备”大赛，中国也开始从国家层面设计区块链的发展道路（发改委委托信通院组织国内主要区块链公司进行区块链的顶层设计的研讨，工信部的信软司也在积极确定区块链的顶层设计机构）。2018 年，区块链及相关行业加速发展，中国将领跑全球进入“区块链可信数字经济社会”，我们正面临区块链重大的产业机遇。

区块链的应用已由开始的金融延伸到物联网、智能制造、供应链管理、数据存证及交易等多个领域，将为云计算、大数据、承载网络等新一代信息技术的发展带来新的机遇，其构建的可信机制，将改变当前社会商业模式，从而引发新一轮的技术创新和产业变革。

编委会成员

顾　　问：张文林、龚体、肖然、廖振钦、万汉阳、楚庆、张辉、潘秋菱、祁峰、伊志权、ZHU PEIYING、刘培、王伟、王小渭、LIAO HENG

研究撰写：张小军、曹朝、胡瑞丰、刘再耀、张亮亮、周瑛达、郭兴民、吴义镇、杜伟、甘嘉栋、WU SHUANG、姜耀国、William Michael Genovese、朱朝晖、刘健

排版设计：杨少青

审　　稿：潘秋菱、张小军、胡瑞丰、刘再耀、周瑛达、曹朝

目 录

1 区块链的兴起

1.1 区块链的起源

探寻区块链的机制和发展，比特币永远是无法绕过的话题。区块链作为一种独立的技术出现，最早可以追溯到比特币系统中。2008 年一个笔名为中本聪的人（或团队）发布了一篇名为《比特币 —— 一种点对点的电子现金系统》的文章，又在 2009 年公开了其早期的实现代码，比特币就此诞生。

抛去比特币价格的跌宕起伏，仅探讨比特币系统本身的设计，可以把它视作一次电子货币在概念和技术上的实验：在传统的电子支付系统（如银行转账或第三方支付等）中，由银行或支付服务提供方来对验证并记录系统中发生的交易，账本在中心机构手中；而比特币在人类历史上第一次实现了去中心化的电子货币发行和交易，即不需要一个中心化的第三方认证机构或账务管理系统对交易进行验证和记录，全网共同维护更新一份相同的账本。比特币的出现使得电子货币系统出现了由传统的“中心化账本+中介”的模式向“公共账本+共识”的模式转变的可能性，而这种转变正是由区块链技术实现的。

比特币白皮书中并没有直接提出“区块链”（Blockchain）这一概念，但其解决交易记录真实有效并不可篡改的方案可以看做区块链系统的雏形：客户端发起交易后向全网广播等待确认，系统中的节点将若干待确认的交易和上一个块的 hash 值打包放进一个块（Block）中并审查块内交易的真实性以形成一个备选区块；随后试图找到一个随机数使得该侯选区块的 hash 值小于某一特定值，一旦找到该数后系统判定该区块合法，节点向全网进行广播，其他节点对该区块进行验证后公认该区块合法，此时该区块就会被添加到链上，进而区块中的所有交易也自然被判定为有效。此后发生的交易则依此法类推链在该区块之后，以此形成一个

历史交易记录不断堆叠的账本链条。任何对链条上某一块的改动将会导致该块 hash 值的变化，进而导致后续块的 hash 值变化与原有账本对不上，因此篡改难度极高。

比特币以上述方案为基础，由数千个分布式节点 7x24 小时不间断运行了近 10 年之久，期间未出现过重大的漏洞。人们逐渐意识到承载比特币运行背后的区块链技术可能极具应用前景，它不该也不会仅限于在电子货币转账中使用。

1.2 区块链的发展路径

电子现金交易的本质是货币（或类货币）资产价值的转移。实际上区块链所带来的分布式记账理念不仅仅能够为电子现金交易服务，它可以被用于处理更广义上的价值转移：各类有形资产和无形资产的所有权归属和流通理论上都可以运用区块链技术进行记录和追踪，并完成点对点的价值交换。这对于社会商业的信息和资产管理而言将会是一次意义重大的革新。

然而由于比特币系统设计的非图灵完备性，其系统无法处理更为复杂的业务逻辑。受比特币启发，于 2015 年左右开发上线的公共区块链平台以太坊则将区块链的应用更进一步，允许开发者在平台上部署智能合约，以处理更为复杂的业务逻辑。智能合约使得通过代码设定好的业务逻辑能够自动按照触发条件执行而无需人为干预，并且合约部署在区块链上公开透明。因此区块链技术可以被广泛的运用在涉及合同处理、数据交换、所有权转移的金融、物联网、物流和共享经济等场景中。

如果从比特币诞生开始计算，区块链技术已有近 10 年的发展历史。目前区块链的发展方向主要可以分为公有链和联盟链：前者以比特币和以太坊为代表，任何人都可以随时加入其中，链上记录对所有人公开；后者则由指定区块链的参与成员组成联盟，成员之间的业务往来信息被记录在区块链中，限定了使用规模和权限，典型代表如 Linux 基金会旗下的开源区块链项目 Hyperledger 等。

表1-1 区块链的发展阶段表

区块链发展阶段	典型事件	作用
2009-2014（区块链 1.0）	比特币系统公布。	区块链技术起源。
2014-2017（区块链 2.0）	以太坊，超级账本等区块链开源项目发布。	区块链协议层和框架层优化，智能合约支持，公有链和联盟链方向出现。
2017-？	商业应用项目爆发出现，但仍未大规模落地。	区块链在不同行业的应用探索，可能向 3.0 进化。

近年来区块链的概念不断被炒热，但技术本身并未大规模落地商用，更多的是一些金融、物流、公益方面的试点。区块链目前在性能、权限和隐私保护、链间互通等方面仍存在诸多问题，其技术还处于发展阶段。相关咨询和分析报告显示，区块链大规模商用将在 3-5 年之后，因此区块链解决方案仍需要各方进行优化，以满足商用需求。

1.3 当前区块链认识上的两大误区

业界对区块链的声音很多，而在这么多针对区块链的声音中，一类声音是极度夸大区块链的功能，而另一类极端的声音是极力抨击区块链存在的缺陷。业界针对新技术需要更客观的评价。

误区一

将比特币等同于区块链。首先当前区块链讲的很热闹，几乎人人都在讲区块链，而更多的是谈论比特币等虚拟货币带来的经济价值，将比特币等虚拟加密货币作为区块链的概念使用，实际上虚拟加密货币仅是区块链中的一种应用形式。目前全球有一千多种虚拟货币，并且数量还在不断增加。虚拟货币（如：比特币）更多的侧重将加密货币作为投资的一种手

段，而对于企业或政府更多关注的区块链则从技术层面探讨如何借助区块链可靠性机制，解决多企业交易安全性问题从而带来商业价值，并试图在更多的场景下释放智能合约和分布式账本带来的科技潜力。

误区二

区块链是一种万能的技术，可替代数据库，替代 Internet。业界一些观点认为区块链颠覆了数据库，或采用分布式数据库取代集中的传统数据库（Oracle、DB2 等）等说法，其实这些只是神化了区块链，区块链主要技术由密码学和共识算法所组成，其中大部分都是已有技术整合而来，并未开辟新的技术体系。区块链技术是对现有技术的一种补充，其在现有的加密技术上，利用分布式账本和共识机制形成在数据流转过程中防篡改的一种机制保障。区块链技术中采用的分布式账本，对于替代数据库来说是不存在的，其不会作为独立数据库使用，因此独立的数据存储仍然存在，并未被替代。区块链无法离开 Internet、数据库等技术，反而脱离这些技术将无法形成技术体系，因此，区块链是 “X+区块链”的技术形态。

2 区块链核心技术及原理机制

2.1 区块链的概念和特征

区块链（Blockchain）是一系列现有成熟技术的有机组合，它对账本进行分布式的有效记录，并且提供完善的脚本以支持不同的业务逻辑。在典型的区块链系统中，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。所有节点共同参与区块链系统的数据验证、存储和维护。新区块的创建通常需得到全网多数（数量取决于不同的共识机制）节点的确认，并向各节点广播实现全网同步，之后不能更改或删除。

从外部来看，区块链系统应具备如下特征：

- **多方写入，共同维护**

  此处的多方仅指记账参与方，不包含使用区块链的客户端。区块链的记账参与方应当由多个利益不完全一致的实体组成，并且在不同的记账周期内，由不同的参与方主导发起记账（轮换方式取决于不同的共识机制），而其他的参与方将对主导方发起的记账信息进行共同验证。

- **公开账本**

  区块链系统记录的账本应处于所有参与者被允许访问的状态，为了验证区块链记录的信息的有效性，记账参与者必须有能力访问信息内容和账本历史。但是公开账本指的是可访问性的公开，并不代表信息本身的公开，因此，业界期望将很多隐私保护方面的技术，如零知识证明、同态加密、门限加密等，应用到区块链领域，以解决通过密文操作就能验证信息有效性的问题。

- **去中心化**

  区块链应当是不依赖于单一信任中心的系统，在处理仅涉及链内封闭系统中的数据时，区块链本身能够创造参与者之间的信任。但是在某些情况下，如身份管理等场景，不可避免的会引入外部数据，并且这些数据需要可信第三方的信任背书，此时对于不同类型的数据，其信任应来源于不同的可信第三方，而不是依赖于单一的信任中心。在这种情况下，区块链本身不创造信任，而是作为信任的载体。

- **不可篡改**

  作为区块链最为显著的特征，不可篡改性是区块链系统的必要条件，而不是充分条件，有很多基于硬件的技术同样可以实现数据一次写入，多次读取且无法篡改，典型的例子如一次性刻录光盘（CD-R）。区块链的不可篡改基于密码学的散列算法，以及多方共同维护的特性，但同时由于这个特性，区块链的不可篡改并不是严格意义上的，称之为难以篡改更为合适。

2.2 区块链的核心技术

2.2.1 分布式账本

分布式账本技术 DLT (Distributed Ledger Technology)本质上是一种可以在多个网络节点、多个物理地址或者多个组织构成的网络中进行数据分享、同步和复制的去中心化数据存储技术。相较于传统的分布式存储系统，分布式账本技术主要具备两种不同的特征：

- 传统分布式存储系统执行受某一中心节点或权威机构控制的数据管理机制，分布式账本往往基于一定的共识规则，采用多方决策、共同维护的方式进行数据的存储、复制等操作。面对互联网数据的爆炸性增长，当前由单一中心组织构建数据管理系统的方式正受到更多的挑战，服务方不得不持续追加投资构建大型数据中心，不仅带来了计算、网络、存储等各种庞大资源池效率的问题，不断推升的系统规模和复杂度也带来了愈加严峻的可靠性问题。然而，分布式账本技术去中心化的数据维护策略恰恰可以有效减少系统臃肿的负担。在某些应用场景，甚至可以有效利用互联网中大量零散节点所沉淀的庞大资源池。

- 传统分布式存储系统将系统内的数据分解成若干片段，然后在分布式系统中进行存储，而分布式账本中任何一方的节点都各自拥有独立的、完整的一份数据存储，各节点之间彼此互不干涉、权限等同，通过相互之间的周期性或事件驱动的共识达成数据存储的最终一致性。经过几十年的发展，传统业务体系中的高度中心化数据管理系统在数据可信、网络安全方面的短板已经日益受到人们的关注。普通用户无法确定自己的数据是否被服务商窃取或篡改，在受到黑客攻击或产生安全泄露时更加显得无能为力，为了应对这些问题，人们不断增加额外的管理机制或技术，这种情况进一步推高了传统业务系统的维护成本、降低了商业行为的运行效率。分布式账本技术可以在根本上大幅改善这一现象，由于各个节点均各自维护了一套完整的数据副本，任意单一节点或少数集群对数据的修改，均无法对全局大多数副本造成影响。换句话说，无论是服务提供商在无授权情况下的蓄意修改，还是网络黑客的恶意攻击，均需要同时影响到分布式账本集群中的大部分节点，才能实现对已有数据的篡改，否则系统中的剩余节点将很快发现并追溯到系统中的恶意行为，这显然大大提升了业务系统中数据的可信度和安全保证。

这两种特有的系统特征，使得分布式账本技术成为一种非常底层的、对现有业务系统具有强大颠覆性的革命性创新。

2.2.2 共识机制

区块链是一个历史可追溯、不可篡改，解决多方互信问题的分布式（去中心化）系统。分布式系统必然面临着一致性问题，而解决一致性问题的过程我们称之为共识。

分布式系统的共识达成需要依赖可靠的共识算法，共识算法通常解决的是分布式系统中由哪个节点发起提案，以及其他节点如何就这个提案达成一致的问题。我们根据传统分布式系统与区块链系统间的区别，将共识算法分为可信节点间的共识算法与不可信节点间的共识算法。前者已经被深入研究，并且在现在流行的分布式系统中广泛应用，其中 Paxos 和 Raft 及其相应变种算法最为著名。对于后者，虽然也早被研究，但直到近年区块链技术发展如火如荼，相关共识算法才得到大量应用。而根据应用场景的不同，后者又分为以 PoW（Proof of Work）和 PoS（Proof of Stake）等算法为代表的适用于公链的共识算法和以 PBFT(Practical Byzantine Fault Tolerance)及其变种算法为代表的适用于联盟链或私有链的共识算法。

工作量证明 POW 算法是比特币系统采用算法，该算法于 1998 年由 W. Dai 在 B-money 的设计中提出。以太坊系统当前同样采用 PoW 算法进行共识，但由于以太坊系统出块更快（约 15 秒），更容易产生区块，为了避免大量节点白白陪跑，以太坊提出了叔（Uncle）块奖励机制。PoS（Proof of Stake）算法最早由 Sunny King 在 2012 年 8 月发布的 PPC（PeerToPeerCoin 点点币）系统中首先实现，而以太坊系统也一直对 PoS 抱有好感，计划后续以 PoS 代替 PoW 作为其共识机制。PoS 及其变种算法可以解决 PoW 算法一直被诟病的浪费算力问题，但其本身尚未经过足够验证。PBFT 算法最早由 Miguel Castro（卡斯特罗）和 Barbara Liskov（利斯科夫）在 1999 年的 OSDI99 会议上提出，该算法相较原始拜占庭容错算法具有更高的运行效率。假设系统中共有 N 个节点，那么 PBFT 算法可以容忍系统中存在 F 个恶意节点，并且 3F+1 不大于 N。PBFT 共识算法虽然随着系统中节点数增多而可以容忍更多的拜占庭节点，但其共识效率却是以极快的速率下降，这也是我们能看到的应用 PBFT 做共识算法的系统中很少有超过 100 个节点的原因。

无论是 PoW 算法还是 PoS 算法，其核心思想都是通过经济激励来鼓励节点对系统的贡献和付出，通过经济惩罚来阻止节点作恶。公链系统为了鼓励更多节点参与共识，通常会发放代币（token）给对系统运行有贡献的节点。而联盟链或者私链与公链的不同之处在于，联盟链或者私链的参与节点通常希望从链上获得可信数据，这相对于通过记账来获取激励而言有意义得多，所以他们更有义务和责任去维护系统的稳定运行，并且通常参与节点数较少，PBFT 及其变种算法恰好适用于联盟链或者私链的应用场景。

2.2.3 智能合约

- 什么是智能合约？

  智能合约（Smart contract ）是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易。这些交易可追踪且不可逆转。其目的是提供优于传统合同方法的安全，并减少与合同相关的其他交易成本。

  智能合约概念可追溯到 20 世纪 90 年代，由计算机科学家、法学家及密码学家尼克·萨博（Nick Szabo）首次提出。他对智能合约的定义如下：“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。” 尼克·萨博等研究学者，希望能够借助密码学及其他数字安全机制，将传统的合约条款的制定与履

行方式，置于计算机技术之下，降低相关成本。然而，由于当时许多技术尚未成熟，缺乏能够支持可编程合约的数字化系统和技术，尼克 萨博关于智能合约的工作理论迟迟没有实现。

随着区块链技术的出现与成熟，智能合约作为区块链及未来互联网合约的重要研究方向，得以快速发展。基于区块链的智能合约包括事件处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约，数据的状态处理在合约中完成。事件信息传入智能合约后，触发智能合约进行状态机判断。如果自动状态机中某个或某几个动作的触发条件满足，则由状态机根据预设信息选择合约动作的自动执行。因此，智能合约作为一种计算机技术，不仅能够有效地对信息进行处理，而且能够保证合约双方在不必引入第三方权威机构的条件下，强制履行合约，避免了违约行为的出现。

- 智能合约的优点与风险

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，智能合约具备以下优点：

a. 合约制定的高时效性：智能合约在制定中，不必依赖第三方权威机构或中心化代理机构的参与，只需合约各方通过计算机技术手段，将共同约定条款转化为自动化、数字化的约定协议，大大减少了协议制定的中间环节，提高了协议制定的响应效率。

b. 合约维护的低成本性：智能合约在实现过程中以计算机程序为载体，一旦部署成功后，由计算机系统按照合约中的约定监督、执行，一旦发生毁约可按照事前约定由程序强制执行。因此，极大降低了人为监督与执行的成本。

c. 合约执行的高准确性：智能合约的执行过程中，由于减少了人为参与的行为，因此利益各方均无法干预合约的具体执行，计算机系统能够确保合约正确执行，有效提高了合约的执行准确性。

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。

无独有偶，2018 年 2 月，新加坡国立大学、新加坡耶鲁大学学院和伦敦大学学院的一组研究人员发布了一份报告声称，他们运用分析工具 Maian，分析基于以太坊的近 100 万个智能合约，发现有 34,200 个合约含有安全漏洞，予黑客可趁之机，可窃取以太币或是冻结资产、删除合约。

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。

- 智能合约的应用

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。

a. 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，并通过编译器转换成字节码(byte code) 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。

b. 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的延伸。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 Fabric 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，对上层业务进行支持。用户链码运行在隔离的链码容器中。

2.2.4 密码学

信息安全及密码学技术，是整个信息技术的基石。在区块链中，也大量使用了现代信息安全和密码学的技术成果，主要包括：哈希算法、对称加密、非对称加密、数字签名、数字证书、同态加密、零知识证明等。本章从安全的完整性、机密性、身份认证等维度，简要介绍区块链中安全及密码学技术的应用。

- **完整性（防篡改）**

区块链采用密码学哈希算法技术，保证区块链账本的完整性不被破坏。哈希（散列）算法能将二进制数据映射为一串较短的字符串，并具有输入敏感特性，一旦输入的二进制数据，发生微小的篡改，经过哈希运算得到的字符串，将发生非常大的变化。此外，优秀哈希算法还具有冲突避免特性，输入不同的二进制数据，得到的哈希结果字符串是不同的。

区块链利用哈希算法的输入敏感和冲突避免特性，在每个区块内，生成包含上一个区块的哈希值，并在区块内生成验证过的交易的 Merkle 根哈希值。一旦整个区块链某些区块被篡改，都无法得到与篡改前相同的哈希值，从而保证区块链被篡改时，能够被迅速识别，最终保证区块链的完整性（防篡改）。

- **机密性**

加解密技术从技术构成上，分为两大类：一类是对称加密，一类是非对称加密。对称加密的加解密密钥相同；而非对称加密的加解密密钥不同，一个被称为公钥，一个被称为私钥。公钥加密的数据，只有对应的私钥可以解开，反之亦然。

区块链尤其是联盟链，在全网传输过程中，都需要 TLS(Transport Layer Security)加密通信技术，来保证传输数据的安全性。而 TLS 加密通信，正是非对称加密技术和对称加密技术的完美组合：通信双方利用非对称加密技术，协商生成对称密钥，再由生成的对称密钥作为工作密钥，完成数据的加解密，从而同时利用了非对称加密不需要双方共享密钥、对称加密运算速度快的优点。

- **身份认证**

单纯的 TLS 加密通信，仅能保证数据传输过程的机密性和完整性，但无法保障通信对端可信（中间人攻击）。因此，需要引入数字证书机制，验证通信对端身份，进而保

证对端公钥的正确性。数字证书一般由权威机构进行签发。通信的一侧持有权威机构根CA(Certification Authority)的公钥，用来验证通信对端证书是否被自己信任（即证书是否由自己颁发），并根据证书内容确认对端身份。在确认对端身份的情况下，取出对端证书中的公钥，完成非对称加密过程。

此外，区块链中还应用了现代密码学最新的研究成果，包括同态加密、零知识证明等，在区块链分布式账本公开的情况下，最大限度地提供隐私保护能力。这方面的技术，还在不断发展完善中。

区块链安全是一个系统工程，系统配置及用户权限、组件安全性、用户界面、网络入侵检测和防攻击能力等，都会影响最终区块链系统的安全性和可靠性。区块链系统在实际构建过程中，应当在满足用户要求的前提下，在安全性、系统构建成本以及易用性等维度，取得一个合理的平衡。

2.3 华为在区块链发展中进行的技术创新

2.3.1 共识算法创新

共识效率是整个区块链对外提供服务的核心能力，实用拜占庭容错算法 PBFT 解决了原始拜占庭容错算法效率不高的问题，将算法复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行，PBFT 完成 3f+1 个节点集群内 f 个节点拜占庭容错，即任一节点收到 2f+1 条消息后可以得到正确的结论（至多有 f 个节点发送恶意错误信息），是联盟链中常用共识算法。

尽管得到广泛应用，PBFT 仍然存在一些缺限。PBFT 算法为了克服 Primary Node 采用了复杂的全量点对点通信来监听各类异常行为，通信复杂度达到 O（n^2）的同时额外增加了大量签名校验，由此带来繁重的系统开销，降低了共识效率、节点扩展性。此外，一旦发生主节点选举，在选主期间 PBFT 将无法正常共识，若新当选的 Primary 节点作弊或者故障，可能会造成连续选主，在此期间，整个区块链系统对外服务能力将会大幅降低甚至无法提供对外服务。

华为区块链采用一种高效、支持拜占庭容错、具有自主知识产权的共识算法，有效改进了 PBFT 算法的上述缺陷。通过改进共识流程，保障了节点故障和切主期间区块链系统对外服务的稳定性。同时通过减少不必要的签名验证、简化共识流程，将通信复杂度从 O（n^2）减少到 O（n），有效提升了共识效率和扩展性。

2.3.2 安全隐私保护

华为区块链安全隐私从以下方面提供更强保障：

- **国密算法**

  国密算法是国家密码局制定标准的一系列算法，随着金融安全上升到国家安全高度，国密算法的应用也越来越广泛，2017 年 11 月 SM2/9 正式进入 ISO/IEC 标准。华为区块链支持国密 SM2/3/4，提供多种加密算法给用户选择，同时满足合规要求。

- **同态加密用户交易隐私保护**

  区块链可以防篡改，去中心化，在非信任的网络运行，但是用户的账本对参与组织是透明的，任何组织都可以访问到相同的数据，如果将用户的隐私的数据放到链上将会放大用户隐私泄露的风险。当前在比特币等公有链系统中，所有的交易信息都是公开的（包括交易金额）。但是，在金融业的交易中，金融交易信息是敏感数据，非业务相关方不能查看，但同时要满足监管机构的监管要求，而大部分的区块链并没有满足隐私性要求。

  华为区块链交易解决方案中：（1）提供同态加密库，对用户的交易数据用其公钥进行加密保护，交易的时候都是密文运算，最终账本中加密保存，即使节点被攻破，获取到账本记录也无法解密；（2）提供范围证明校验，背书节点能够对密文进行背书，无需解密就能校验交易的正确性，从而识别出恶意交易风险，保证了智能合约的正确执行。华为开发出适用于 Hyperledger Fabric 平台的保密交易系统，通过改良的算法，比起使用传统的加法同态加密与基于环签名的范围零知识证明，性能大幅提升。

- **零知识证明**

  零知识证明能够在不向验证者提供任何有用的信息情况下，使验证者来相信该结论是正确的，证明过程中不用向验证者泄露被证明的消息。华为区块链将会提供零知识证明能力，对用户的隐私数据进行保护，减少用户隐私泄露风险。

- **智能合约安全**

  当智能合约运行错误或者编程错误时，就会导致“DAO”的事件，从而让用户遭受巨大损失，华为区块链可提供智能合约检测工具，防止恶意的企图通过智能合约漏洞入侵用户数据的行为，同时将提供安全容器，持续监控容器的运行状态，若发现漏洞，进行有效的隔离，严格对容器的访问权限进行控制，从而保证合约安全运行。

- **共识安全**

  华为区块链将提供基于硬件的共识算法，使用形式化验证保证共识机制的安全，同时可以提高共识效率，增加网络的稳定性。

- **账本安全**

  每个节点的本地账本可能会被篡改，如果出现大部分节点的本地账本都被修改，就可能造成 51%的攻击。 华为区块链将提供基于硬件的保护机制，对本地账本的机密性和完整性保护，防止账本被篡改。

- **通信端到端安全**

  通用 TLS 通信只能保护应用与应用之间的安全，如果启动 TLS 之前，就已经被攻击，TLS 的保护就失效。华为区块链将提供基于硬件的解决方案，端到端的保证区块链节点间的通信安全。

2.3.3 离链通道

单位时间内交易处理能力仍是区块链大规模应用的主要瓶颈之一。受限于区块链的分布式架构特性，节点间不均等的计算能力，不同的网络状况等因素，全网共识往往无法快速达成，从而导致交易速度难以提升。现阶段比特币网络每秒仅能处理约 7 笔交易，支持智能合约的以太坊交易处理速度约为每秒 15 笔。相比之下，中心化服务器支持的 VISA 系统峰值吞吐率可达 56,000 笔，支付宝在 2017 年双十一期间则达每秒 256,000 笔峰值吞吐率。交易拥堵，交易费攀升已极大限制区块链的规模性应用。

区块链社区对交易扩容方案的争论与尝试由来已久，现有的主要方案包括区块扩容，共识算法改良，安全硬件(TEE)辅助，隔离见证，闪电网络，交易/状态分片，多层子链等。但

无论哪种方案都难以同时兼顾去中心化，可扩展性，安全性三个关键需求。值得注意的是区块链具有应用强相关性，在特定应用场景仍可找到各要素间的平衡点以满足总体业务需求。

在大规模 DAPP（Decentralized APP）应用中，往往小额支付占据了大部分交易请求，而小额交易并无必要在主链及时获得确认，例如共享经济中广泛存在的小额支付场景。如果将海量小额交易在链下通道处理，交易过程中不与主链交互，而在交易通道关闭或交易方退出时才请求主链记录交易最终状态，这将极大缓解主链的处理压力，这也是离链微支付通道的设计思想。 典型应用包括比特币框架下的闪电网络(Lightning Network)和以太坊智能合约框架下的雷电网络(Raiden Network)。 离链通道涉及到“链上锁定-链下执行”等一系列操作，其中交易双方的状态变化(资金分配比例)与交易执行过程由链上合约监督执行。

华为开发出适用于 Hyperledger Fabric 平台的离链通道交易系统， 通过交易方高效安全的握手协议，实现用户间单通道 2,000+ TPS 的交易性能。随着离链交易通道数的增加，可进一步提升系统在单位时间内交易处理能力。

3 区块链国内外产业发展现状

3.1 区块链相关产业政策现状

中欧在区块链产业政策中逐渐引领全球，欧盟在 2018 年 2 月已成立欧洲区块链观察论坛，主要职责包括：政策确定，产学研联动，跨国境 BaaS（Blockchain as a Service）服务构建，标准开源制定等，并且在 Horizon 2020 投入 500 万欧作为区块链研发基金（在 2018 年 12 月 19 日前），预计三年内（2018-2020）区块链方面投资将达到 3.4 亿欧元。而美国则由于各州之间政策不一，虽然区块链在美国初创企业中仍然是热潮，但产业政策推动一直较慢。中东地区以迪拜为首在引领区块链的潮流，由政府牵头，企业配合以探索区块链的新技术应用。亚太区域日韩也相对活跃，日本以 NTT 为主，政府背后提供支撑，韩国以金融为切入点探索区块链应用。

中国国务院印发《“十三五”国家信息化规划》，区块链与大数据、人工智能、机器深度学习等新技术，成为国家布局重点。中国人民银行印发了《中国金融业信息技术 “十三五” 发展规划》，明确提出积极推进区块链、人工智能等新技术应用研究，并组织进行国家数字货币的试点。在 2017 年 10 月，工信部发布《中国区块链技术和应用发展白皮书》，这是首个落地的区块链官方指导文件。

各地政府，特别是沿海地区纷纷成立区块链实验地、研究院。目前，深圳、杭州、广州、贵阳等地政府都在积极建立区块链发展专区，给予特别扶植政策。其中广州在 2017 年 12 月正式发布广州区块链 10 条策略，在黄浦区和开发区打造区块链企业技术创新区。深圳在 2018 年 3 月由深圳市经济贸易和信息化委员会发布《市经贸信息委关于组织实施深圳市战略性新兴产业新一代信息技术信息安全转型 2018 年第二批扶持计划的通知》，区块链在扶

持方向之列，这是继广州、贵阳、青岛、杭州之后，国内第 5 个地方政府，出台的关于区块链的扶持政策。

3.2 区块链在开源领域的发展现状

超级账本（Hyperledger）

超级账本（Hyperledger）是由 Linux 基金会于 2015 年发起的推进区块链数字技术和交易验证的开源项目，吸引了包括 IBM、英特尔、Fujitsu、Cisco、华为、Redhat、Oracle、三星、腾讯云、百度金融等众多公司参与，目前已经有超过 200 家会员单位。Apache 基金会创始人 Brian Behlendorf 担任超级账本项目的执行董事。

超极账本项目的目标是让成员共同合作，共建开放平台，满足来自多个不同行业的用户案例，并简化业务流程。超级账本旗下有多个区块链平台项目，包括 IBM 贡献的 Fabric 项目，Intel 贡献的 Sawtooth 项目，以及 Iroha、Burrow、Indy 等。

华为是 Hyperledger 重要成员，不仅在 Hyperledger Fabric 和 Sawtooth Lake 项目贡献大量代码，担任国内仅有的项目 Maintainer 职位，而且也为 Hyperledger 社区贡献了区块链性能测评工具 Caliper 项目。

企业以太坊联盟（Enterprise Ethereum Alliance）

2017 年 2 月，企业以太坊联盟（EEA）正式成立。联盟轮转董事会的创始成员包括埃森哲、桑坦德银行、BlockApps、BNY 梅隆、芝商所、ConsenSys、英特尔、摩根大通、微软、Nuco、IC3。截至 2018 年 2 月，企业以太坊联盟已经吸引了超过 150 家成员加入。

企业以太坊联盟旨在合作开发使企业更容易地使用以太坊开发区块链应用的标准和技术。企业以太坊联盟以提高以太坊区块链的隐私、保密性、可扩展性和安全性为重点，另外还将探索跨越许可以太坊网络、公共以太坊网络以及行业特定应用层的混合架构。

以太坊是由 Vitalik Buterin 开发的一种非常流行的能够部署去中心化应用的公有链技术，但目前其还不能满足企业开发联盟链应用的需求。很多企业各自基于以太坊技术进行了区块链联盟链应用探索和技术改进。企业以太坊联盟的成立，能够联合各个利益集团、公

司、用户等共同出谋划策，使得以太坊区块链能够满足企业级应用需求，繁荣整个以太坊生态系统。

3.3 区块链在标准领域的发展现状

ITU-T

ITU-T（国际电信联盟标准化组织）于 2016 至 2017 年初，SG16（Study Group）、SG17 和 SG20 分别启动了分布式账本的总体需求、安全，以及在物联网中的应用研究。成立三个焦点组 Focus Group（分布式账本焦点组（FG DLT）、数据处理与管理焦点组（FG DPM））、法定数字货币焦点组（FG DFC），分别针对区块链与分布式账本技术应用与服务研究，基于区块链建立可信任的物联网和智慧城市数据管理框架，基于数字货币的区块链应用展开标准化工作。华为担任分布式账本焦点组（FG DLT）架构组主席和数据处理与管理焦点组（FG DPM）区块链组主席。

CCSA

CCSA（中国通信标准化协会）两个委员会分别成立了子组和项目：

CCSA TC10（物联网技术工作委员会）2017 年 10 月成立物联网区块链子组：负责区块链技术在物联网及其涵盖的智慧城市、车联网、边缘计算、物联网大数据、物联网行业应用、物流和智能制造等领域的应用研究与标准化，由中国联通技术专家担任组长，华为技术专家担任副组长。

CCSA TC1（互联网与应用技术工作委员会）下区块链与大数据工作组完成两个区块链行业标准：《区块链：第 1 部分 区块链总体技术要求》和《区块链：第 2 部分 评价指标和评测方法》，华为积极参与其中。

JPEG

2018 年 2 月第 78 届 JPEG 会议期间，JPEG 委员会组织了关于区块链和分布式账本技术及其对 JPEG 标准影响的特别会议。考虑到区块链和分布式账本等技术对未来多媒体的潜在

影响，委员会决定成立一个特设小组在多媒体环境下探索与区块链技术相关的用例和标准化需求，以支持专注于图像和多媒体应用的标准化工作。

IETF

在 2017 年 6 月 IETF99 会议上成立“Decentralized Internet Infrastructure Proposed RG(Research Group)，计划研究区块链架构和相应的标准，2018 年 IETF 在区块链上将可能更多的关注区块链的互联互通的标准的落地发展。

IEEE

成立区块链工作组 P2418（ Standard for the Framework of Blockchain Use in Internet of Things (IoT)），重点针对区块链在 IoT 场景标准的研究，考虑未来区块链在 IoT 场景下的接口对接标准的确立。

ISO

ISO TC307（区块链和分布式账本技术委员会）成立 5 个研究组 SG（参考架构、用例、安全、身份、智能合约），制定全球区块链标准和相关支持协议。

W3C

W3C 启动 3 个 CG（Community Group），其一是 Blockchain CG：研究和评价与区块链相关的新技术以及 usecase（如跨银行通信），基于 ISO20022 创建区块链的消息格式，并孵化 FlexLedger 项目，重点关注区块链间的数据交互性；其二是 Blockchain Digital Assets CG：讨论在区块链上创建数字资产的 Web 规范；其三是 Interledger Payments CG：连接世界范围的多个支付网络（ledger）。

3.4 区块链产业联盟发展现状

R3

2015 年 9 月，R3 区块链联盟由 R3CEV（R3 Crypto Exchange Venture）公司发起，吸引了众多金融机构的参与，包括富国银行、美国银行、德意志银行、汇丰银行、摩根史丹利、花旗银行等。目前 R3 联盟已经吸引了超过 60 家会员。R3 致力于为银行提供区块链技术以

及建立区块链概念性产品。2016 年，R3 宣布了其为金融机构量身定做的区块链技术平台项目 Corda，并于 2017 年将 Corda 项目代码开源。

CBSG 运营商区块链联盟（Carrier Blockchain Study Group）

2017 年 2 月，美国电信运营商 Sprint、美国加州区块链初创公司 TBCASoft、日本软银集团合作，成立 CBSG，使用 TBCASoft 开发的一个平台将 Sprint 的系统连接在一起。利用 Sprint 底层核心网络，构建 TBCSoft 区块链平台层，多个基站子系统（BSS）接入区块链平台，在多个应用之间共享账本。

CBSG 在跨运营商的支付平台系统上完成充值、移动钱包漫游、国际汇款和物联网支付。目前为止，该联盟已经成功测试了移动支付系统，并通过该平台为不同运营商的预付费电话充值。将来，该组织会推出连接计算、个人认证和债务清算的应用程序。在 2018 年的 MWC 上 CBSG 宣布又增加了 5 家成员：KT，LGU+，Telefonica，FLDT 和 Etisalat，成员数从原有 4 家发展到 9 家。华为已与其保持深入交流。

TIoTA 可信物联网联盟（Trusted IoT Alliance）

2017 年 9 月，思科、Bosch、ConsenSys、IOTA 等公司联合成立，成员还包括 BNY Mellon、U.S.Bank、BigchainDB 等。可信物联网联盟将会建立基于区块链的、可信赖的物联网生态系统，提升物联网的安全性及可信性，同时也将制定开源区块链协议的标准，来加强物联网的安全性。根据路线图，可信物联网联盟将会支持基于超级账本、比特币和以太坊技术的区块链实现。

BiTA 区块链货运联盟（Blockchain in Transport Alliance）

BiTA 成立于 2017 年 8 月，成员包括联邦快递、UPS、Penske、GE 运输、SAP、Salesforce、京东物流等，目前已经超过 100 家。BiTA 整合货运及物流行业各方，共同探讨区块链在货运行业的应用，开发货运行业的区块链标准，从而提高货运流程的透明度及效率，使该行业变得更加先进。

B3I 区块链保险行业倡议（Blockchain Insurance Industry Initiative）

2016 年 10 月，荷兰全球人寿保险公司（Aegon）、德国安联保险集团（Allianz）、德国慕尼黑再保险公司（Munich Re）、瑞士再保险公司（Swiss Re）、苏黎世保险集团有限公司（Zurich Insurance Group）五大保险巨头联合发布保险行业区块链倡议 B3I，旨在研究区块链在保险业的可行性，并开发基于区块链的保险概念证明。

中国区块链技术和产业发展论坛

2016 年 10 月 18 号由工信部信息化和软件服务业司、国家标准委工业标准二部指导在北京成立，联盟凝聚政、产、学、研等各方资源，跟踪研究区块链技术和应用发展趋势，研究标准，构建我国区块链发展路线图，同时组织对外交流。

金融区块链合作联盟

2016 年 5 月，深圳市金融科技协会等二十余家金融机构和科技企业共同发起成立，目标是在 3 至 5 年内研发一条或多条金融区块链。目前华为与华夏银行、广发银行等多家企业参与，致力于金融领域的区块链的研究和产业共识的建立。

可信区块链联盟

为落实《“十三五”国家信息化规划》，搭建政产学研合作平台，推进区块链技术与实体经济深度融合，在工业和信息化部的指导和支持下，中国信息通信研究院牵头成立“可信区块链联盟”。目前联盟约 150+企业参与，华为、京东金融、智链、腾讯、中国移动、中国电信等都参加联盟。华为作为副理事长单位参与，依托信通院打造的合作平台，支撑国家在区块链的顶层设计，协助构建和谐共赢的产业环境。

4 区块链的典型应用场景

华为目前关注的区块链的应用场景主要如下（包含但不限于）：

-	典型场景	说明
数据	数据存证/交易	搭建可信的数据交易平台，实现数据资产的登记、交易、溯源，帮助企业进行数据资产变现。
	身份认证	实现 IOT 设备/用户的接入鉴权、固件管理等，提高系统安全性。
行业应用		
IOT	新能源	搭建新能源点对点交易系统，实现可信交易和价值转移。
	供应链溯源	实现数据共享，打通各环节流程，提高数据透明性、可追溯性。
	车联网	共享汽车的里程、速度等信息，供相关利益方（保险公司、车厂等）获取。
电信	多云多网协同	多云+多网可信接入，使能“多网+多云”云业务全球无缝漫游。
金融	供应链金融	金融系统进入企业的业务系统，实现对供应链上下游企

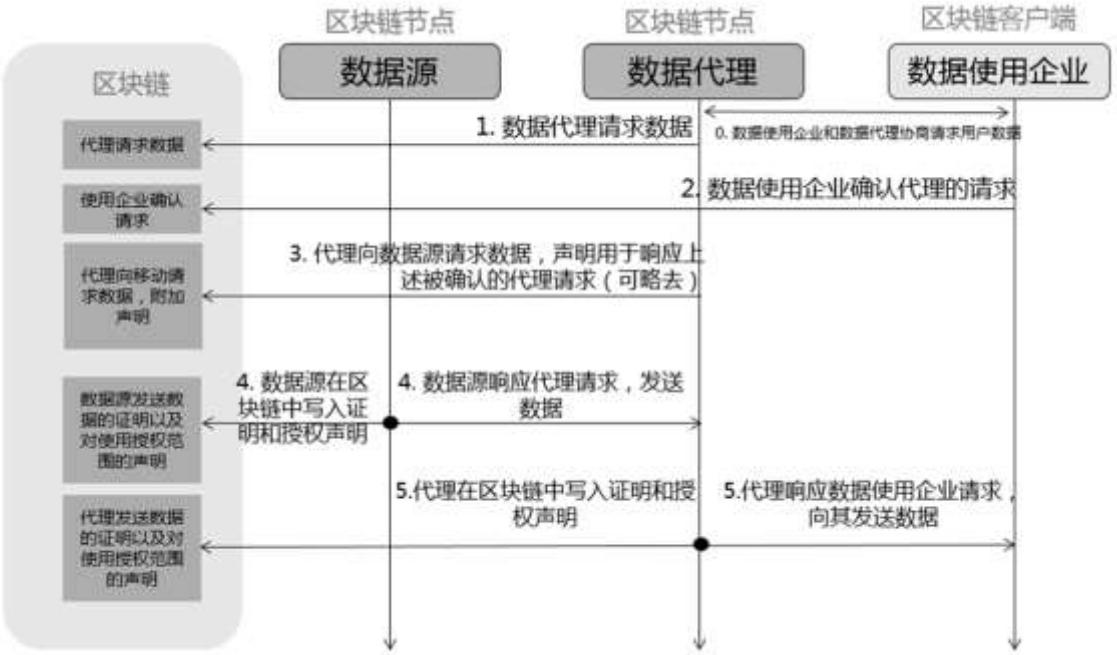
-	典型场景	说明
		业的可信放贷。
	普惠金融	构建个人的可信信息，降低身份审核成本，提升金融业务的人群覆盖面，促进整个经济的发展。

4.1 数据交易：实现数据交易的过程透明、可审计，重塑社会公信力

数据是未来以互联和机器学习为主的经济中最重要的成分，AI 算法分析数据会产生许多改变世界的发现。而对于数据收集能力有限的企业，数据交易将是一个互惠互利的工作，可以促进公司的创新，创造新的收入来源。然而由于目前数据交易市场上存在数据非法倒卖，信息透明度低，易被篡改等问题，导致数据交易的规模受限。

区块链的去中心化、安全性和不可篡改可追溯性，可以让参与主体之间建立信任，推进数据交易的可持续大幅增长：数据所有权、交易和授权范围记录在区块链上，数据所有权可以得到确认，精细化的授权范围可以规范数据的使用。同时，数据从采集到分发的每一步都可以记录在区块链上，使得数据源可追溯，进而对数据源进行约束，加强数据质量。基于区块链的去中心化数据交易平台，可以形成更大规模的全球化数据交易场景。

图4-1 基于区块链的数据交易确权示意图



特别是在物联网领域，分布广泛的物联网设备、传感器等会收集大量的数据。去中心化数据交易网络能很好的支持分布、实时和精细化的数据交易，可以成为物联网领域数据交易的媒介；同时它也能引入信任度，持续保持透明度，很好的支持物联网领域数据交易生态系统的参与主体，包括数据采集，存储，交易、分发和数据服务各个流程的参与者；最后，去中心化数据交易网络也需要在可扩展性，交易成本和交易速度方面有突破，才能加速推动物联网领域数据市场的商用化。

4.2 身份认证：验证身份的合法性，加速数字化社会发展

身份及接入管理服务是区块链技术应用的一个重要领域，不仅如此，由于区块链技术可以带来高可靠性、可追朔和可协作等特质，使得其在身份及接入管理服务的应用领域具备成为基础技术的潜力。

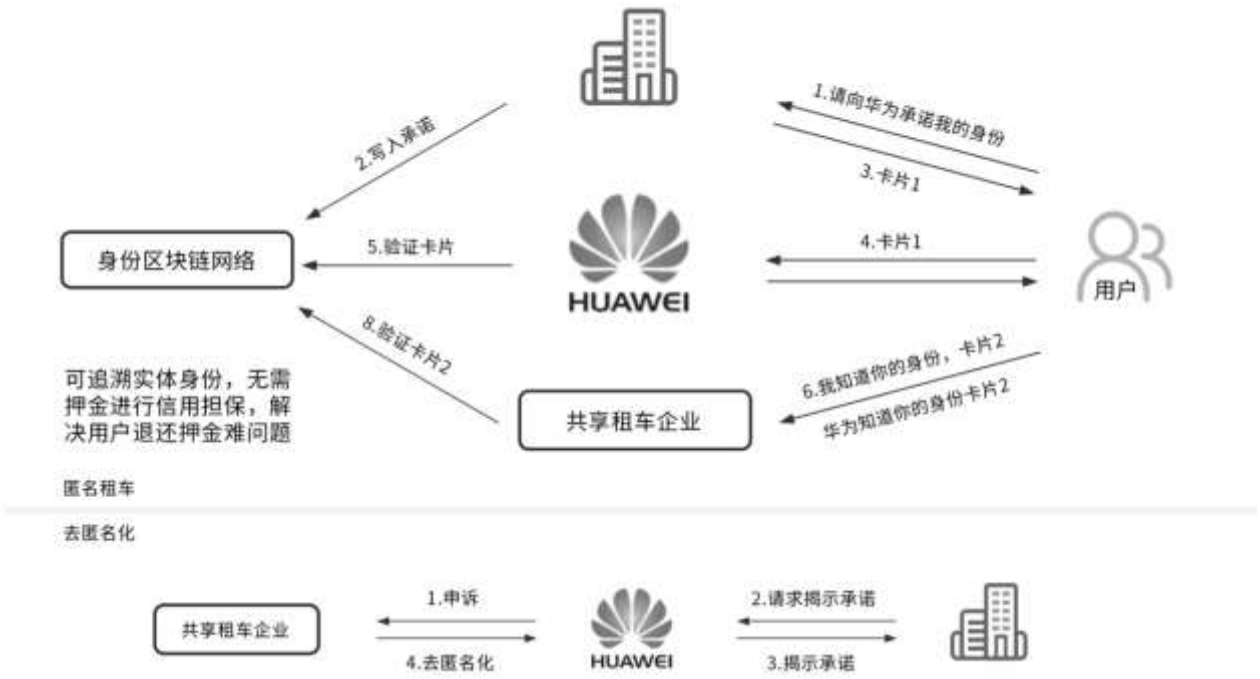
伴随着数字化进程的加速，身份及接入管理服务的应用领域将越来越广泛，包括互联网、物联网、社会和经济生活等。在这些应用领域中，身份及接入管理服务的典型作用是保障具备合法身份的用户或设备可以安全、高效的接入和享受服务。

身份及接入管理服务在各个应用领域中所处的位置至关重要，但目前该服务也一直面临着隐私泄露、身份欺诈以及碎片化等问题，给用户、设备和系统均带来极大的挑战。

区块链技术的引入和发展，为进一步解决上述问题提供了新的思路。将区块链技术应用到身份及接入管理服务中，将有可能形成一种协作的、透明的身份管理方案，有助于企业、组织更好的完成身份管理和接入认证。

华为区块链技术在身份及接入管理服务的应用，将依托新的硬件、软件和区块链平台等的配套支持，为企业、组织提供专业、安全、高效的身份和管理服务，身份认证的应用示例如下图。

图4-2 华为区块链自主身份认证方案



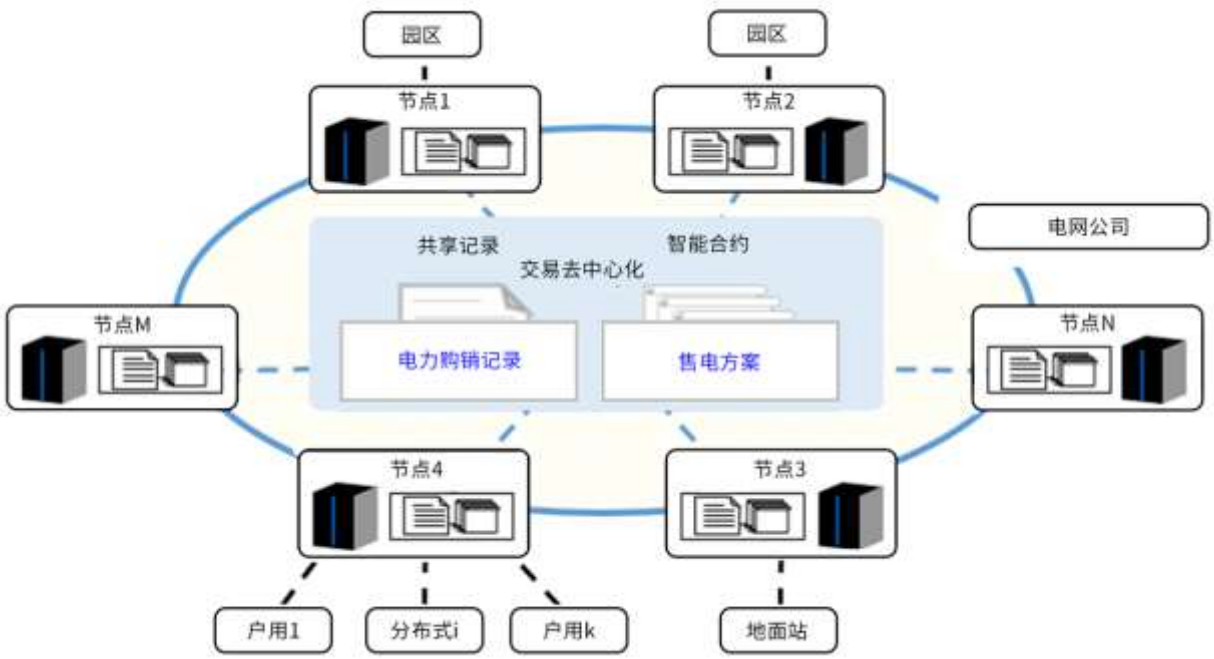
4.3 新能源：打造清洁能源交易信任基石

在新能源领域，区块链技术的应用正在改变着现有的行业结构，降低交易成本，并保留更有效的记录，实现能源互联网从数字化向信息化最后向智能化发展的路径。随着分布式光

伏、储能的成本大幅降低，以区域自治为核心的能源微网社区将逐步凸显经济性。同时，诸如太阳能这类新能源往往具有分布式的特点，发电厂及住户都可以使用太阳能板来进行储能，能源认领可以发生在生产者和消费者之间，因此可以通过区块链和智能电表，对不同主体的发电量进行计量和登记以形成一个不可篡改的发电量账本；同时通过智能合约来实现多余电力的点对点认领和交易。另一方面，区块链还可以促进新能源给社会带来巨大的公益和环保价值。通过区块链和智能电表，对不同主体的发电量进行计算和登记以形成一个不可篡改的清洁电力发电量账本，相关环保和公益机构完全可以在这笔交易在区块链中被验证有效时向用户和发电厂发放清洁能源生产和使用证书，以鼓励双方生产和使用新能源的行为。

华为在某新能源区块链项目中，通过区块链技术的使用，用户可以清晰的查阅到他们的每一笔交易记录，了解所使用的每一度电具体来源于哪个发电站的哪个光伏发电板，并能够根据该发电站的电价及剩余可用发电量，自主选择自己的供电来源。智能合约直接配对电站和用户间的认领。通过认领清洁电力，用户获得权威电子证书，证明其对节能减排做的相关贡献。而对于发电企业来讲，则可以根据用户所提交的用电申请，动态计算各电站的供需状态，及时调整发电策略以及价格。

图4-3 华为区块链在新能源点对点认领方案



4.4 车联网：用区块链实现信息准确共享，构建新经济模式

车联网是基于网络连接、车载传感器数据收集，配合云端的设备管理、大数据分析等技术的融合，并加上大量的应用创新而形成的一种综合性技术。也正是这些技术和应用的不断融合和积累，使得汽车的经营维护模式逐步实现了巨大的转变，由最初的单产品服务，到现在的多方协同维护，再到可预见的未来的生态化价值链。

在这个发展过程中，越来越多经营实体加入到这个围绕着车辆完整生命周期服务的链条中，并且互相之间将形成越来越密切的关系，保险与 4S 店的配合是典型的例子。但目前在这些相互配合中，信息散落在各个环节且形式各异，在交互过程中的信息传递也只依赖于双方的信用和人工保证，也就是信息的完整性、一致性、可靠性和交互的效率等方面存在一定的限制，这同时也提高了更多的经营实体、第三方应用加入到这个价值链的门槛。具体来说，车联网存在如下特点：

- **数据来源广**

  大量的车载传感器、网络连接、云端服务，使得数据的获取/分析呈现自动化，分布式的特点。

- **多方参与**

  包括用户/企业、车厂、4S 店、保险、共享车企、二手市场、车辆管理部门、执法部门、创新应用开发商等等。

- **利益不一致且无单一可信方**

  例如用户、保险、4S 店之间存在一定的利益博弈。虽然有途径进行权威仲裁，但往往是事后的、冗长的流程。

- **需客观取证**

  如事故记录等客观事实会被多方采用。

- **大量流程交互**

  如一次交通肇事、一次车辆交易、一次用户的服务请求，往往都涉及多方的流程交互，一个统一的数据交互机制将大大提升其效率。

可以发现，区块链技术所倡导的解决问题的场景和优势与上述车联网特征不谋而合。利用区块链，可以通过数据防篡改和可追溯的统一账本来记录车辆整个生命周期的信息，该账本在各参与方之间共享（参与方既可以是信息提供者，又可以是信息使用者），实现去中心化的信息互通。同时，结合智能合约、链上链下数据互通等更前沿的技术，可实现整个价值链上各种流程的自动化，进一步提升效率。例如基于车辆的生命周期信息，可以考虑将区块链用于出厂/维修/改装/维护、故障权责定界、保险理赔、二手车车况取证等场景。

由于涉及从用户到企业再到监管部门等不同参与方，数据隐私是区块链应用于车联网的关键挑战，这包括技术和非技术两方面。技术上，需要通过加密、授权等相关机制，使得某个流程相关的数据只有参与该流程的实体可以访问，而不是无约束地可访问任何链上数据；非技术层面，用户是否同意让自己车辆的数据在多个实体之间共享，例如让保险公司了解汽车的维修记录等。面对这些问题，在初期可优先考虑车队管理、共享汽车、车企内流程互通等隐私低敏感场景。

4.5 供应链溯源：树立公信力，构建真实交易

每年的 315 打假仅是打假过程的冰山一角，产品溯源防伪仍是目前社会和企业的主要难题。以食品为例，虽然有绿色食品标识，但因为人为因素在整个供应链中参与过多，导致对中间环节的数据可信度存在较大疑问，这会对社会和企业的公信力产生很大的影响。食品是否是绿色无污染的，高端艺术品/奢侈品是否为赝品等一系列问题仍然摆在社会面前。

区块链技术依托其具有的数据不可篡改、交易可追溯以及时间戳的存在性证明机制，可以很好的解决供应链体系内各参与方在数据被篡改时产生的纠纷，实现有效的追责和产品防伪。

供应链溯源分为三大类：第一类为食用产品（肉类、蔬菜、水产品、婴儿奶粉、中药材等）；第二类为高档消费品（名贵酒类）和高端艺术区（文物、珠宝等）；第三类为文件证书产品（房产证、学历证等），实现供应链上下游企业全部纳入追溯体系，构建来源可查、去向可追、责任可究的全链条可追溯体系。

以牛奶溯源为例：目前牛奶溯源主要有奶牛业主，奶牛饲料提供商，奶牛灌装厂商，物流方，监管方，售卖方（商场超市）。首先奶牛业主通过第三方传感器，获得奶牛日常的喂养过程以及牛奶的检测数据并记录在账本中，针对这些数据，监管部门或防疫部门会根据其数据给予奶牛业务提供相应的支撑，并补充到分布式账本中。奶牛饲料提供商给奶牛业主提供的饲料情况的数据上链后，可有效对非法饲料跟踪和定责。再通过灌装厂商的灌装流程数据，以及物流方的数据，从而获知牛奶的运输中的保鲜度。通过售卖方，可以方便普通用户通过终端应用获取想要购买奶粉的整个生产和售卖流程，从而杜绝非法产品，有效构建政府公信力，同时基于数据的共享，各方可以知道相互的需求，实现更为有效的合作互赢。当然在牛奶生产过程中，发现数据不达标则会马上预警进行调整，并且不达标的数据无法生成平台认证的质量签名，对应牛奶将被拒绝销售，且数据超标的，将及时进行销毁，从而保障牛奶品质。同时监管部门对不能认真保障牛奶质量的业主，给予相应的惩罚，取消其奶牛饲养资格，并将业主加入非诚信人员名单，对其后续的经营资质产生很大影响形成督促作用，目标是形成自治的良性循环，避免人为弄虚作假。

4.6 运营商云网协同：解决运营商网络碎片化，构建新商业模式

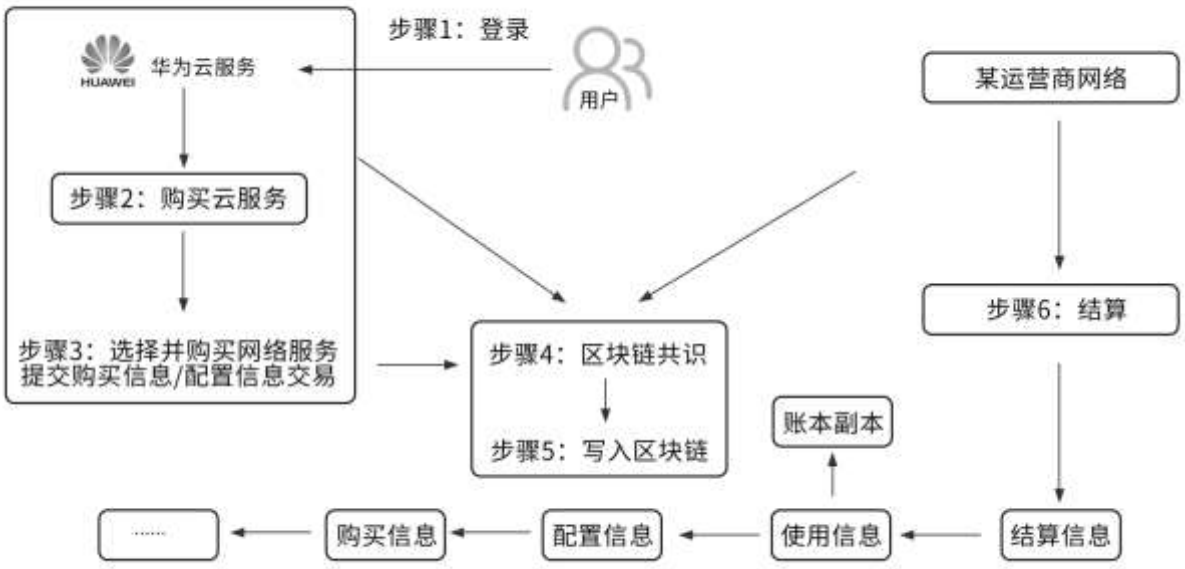
传统运营商基于”烟囱式的网络即业务”架构，业务和网络都是运营商经营，网络是支撑系统，业务与网络之间的费用内部结算，但随着 ICT 融合，通信产业从封闭走向开放，业务提供者除了运营商之外，还包括了大量 OTT 类云服务商和虚拟业务提供商。为支撑新业务生态的需求，运营商网络需要云化重构，实现类似云计算 IaaS/PaaS（Infrastructure as a Service/ Platform as a Service）一样灵活、弹性、自动化的网络即服务（NaaS）的能力。这些能力可以有偿的开放给各云服务商和虚拟业务提供商，实现网络能力变现。区块链可以在不同节点之间建立信任、随着运营商网络从封闭的内部结算方式向货币化的对外服务转型，可以引入区块链技术，为多云、多网、多端之间建立互信的新型交易模式。

根据英国电信（BT）对企业客户的调研显示，90%的企业希望能获得“云网一体化”的服务，以保障端到端的 SLA(Service-Level Agreement)、安全，获取端到端的性能报告、实现

端到端的管理和故障诊断能力。云网系统需要支持从任意一个云服务或者网络业务的销售入口登入，可以购买到任意一家的云服务或网络业务的功能，而不用多次登录不同的入口。

基于以上诉求，可以设计一种基于联盟链的云网业务方案：对联盟内企业进行“多云+多网”的销售进行授权认证，对云和网的销售记录、配置情况进行记账和追溯。以云服务侧购买网络为例：云服务侧向区块链提交购买/配置信息请求，而网络服务侧验证请求并确认请求，云服务和网络服务侧达成共识并写入区块链，至此购买成功。在结算上，可根据区块链上的购买信息、配置更改信息、使用信息进行结算，同时保证账本的一致性，并支持实时结算。

图4-4 云网协同区块链解决方案



4.7 供应链金融：有效减少金融风险，拓展金融业务发展

华为关心区块链在金融行业的应用场景，因为这与我们通过“云、管、端”为金融服务推动数字化转型和成熟化的核心战略直接匹配，此外，区块链加速了信息的安全分发，呈现，传输和处理。从区块链技术中受益最多的往往是那些参与者之间信任度较低、交易记录安全性和完整性要求较高的行业，而金融业正是其中之一。相关咨询报告显示区块链或分布

式账本技术每年可为金融行业节省成本 50-70 亿美元，这种成本的降低主要来自于区块链对现有业务的改进，如跨境支付价值链的改善、对账流程的优化、用户身份认证/反洗钱流程的效率提升和供应链金融以及普惠金融中的信息共享等。

“区块链+供应链金融”是区块链在金融领域的最佳应用场景之一，具有广阔的市场空间。供应链金融具有系统性、结构性的业务理念，决定了信息流是供应链金融风险把控的关键。如何获取真实、全面、有效的数据，既是供应链金融风控的基础，又是风控的难点，通过区块链的分布式账本等技术可以在供应链参与中的众多企业、众多金融机构间搭起一张可信的信息网络，从企业经营信息的源端获取信息，然后通过区块链达到端到端的信息数据透明、不可篡改，所有参与方都通过一个去中心化的记账系统分享商流、物流、资金流信息。银行根据真实的企业贸易背景、实时产生的运营数据开展授信决策，缩短资料数据收集、校验、评估的作业时间，降低风险成本，提升决策的精确性和效率。而企业通过供应链金融可以获得更低的贷款成本，更快速迅捷的金融服务，帮助业务的顺利开展和拓广。

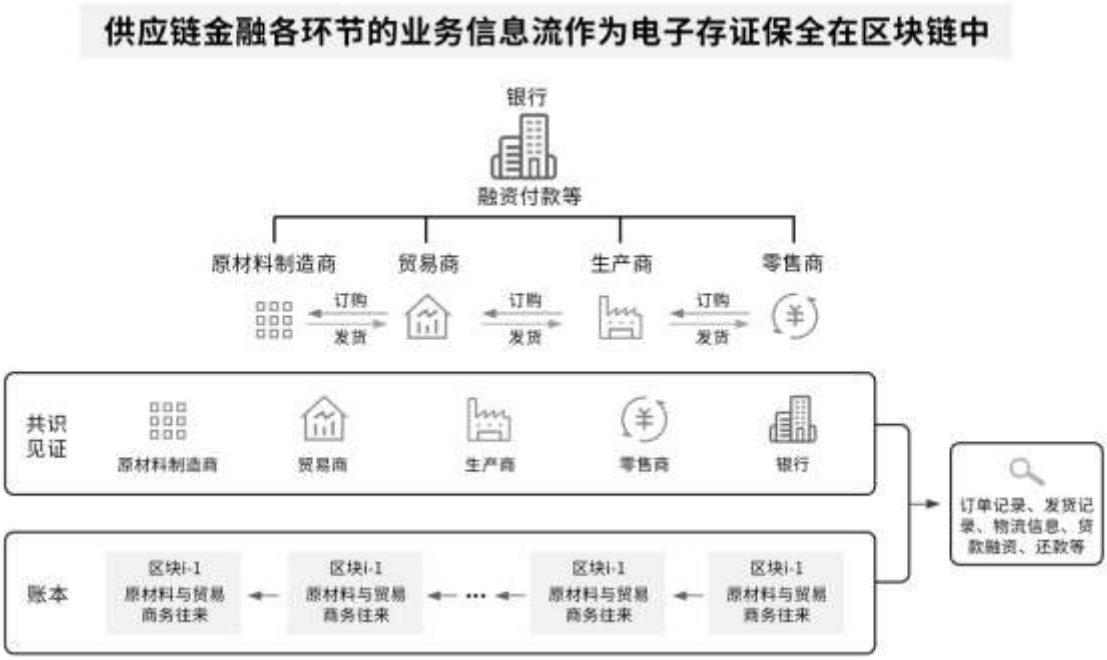
具体而言，区块链技术可以为供应链金融在以下方面提供强有力的支持：

- 通过区块链的不可篡改性，记录供应链金融中上下游企业和周边企业的资金流、物流、商流过程，降低供应链金融过程中，可信数据采集、传递的难度；为金融机构获取第一手的供应链信息提供便利。如果企业广泛部署物联网终端，结合企业信息化系统的进销存信息，可以真实的勾勒出企业的运营情况与资产情况；企业透过企业网银、银企直联等渠道与上下游企业产生资金往来，提供真实的财务资金信息；这些信息将帮助金融机构在进行贸易融资、仓单贷款、应收账款贷款过程中极大简化信用评估流程与成本，以此降低企业融资的成本，提供融资的效率；
- 通过“智能合约”等技术手段，为企业间“合同信任”关系之外，添加新的保障措施，简化企业间互担保、风险分摊、回购、履约等经营行为的流程，降低违约纠纷处理的时间成本和资金成本。以合同融资为例，合同的买方与卖方建立起中长期的供应关系，采购方的销售数据衍生出对原材料的采购需求的评估数据，市场的真实供需关系是融资回收的第一保障；若采购方企业提供风险缓释措施，在风险条件触发后，采购方是否按指令进行回购、退款等风险补偿履约措施，直接影响融资贷款是否产生不良资产。现行的操作中，上述履约约束主要来源于“合同信任”，但履约过程中可能存在法律争议，后

期将增加法律纠纷的处理时间及成本。引入区块链“智能合约”，将上述合同约定事项上链，使其变为自动触发与操作，从技术的角度弥补履约中的意外过程和主观违约可能，保障融资安全。

供应链金融中采用区块链技术的流程示意如下：

图4-5 供应链金融区块链解决方案



5 华为区块链的方案及特点

5.1 华为云区块链服务（BCS：Blockchain Service）

华为云区块链服务 BCS 是基于开源区块链技术和华为在分布式并行计算、PaaS、数据管理、安全加密等核心技术领域多年积累基础上推出的企业级区块链云服务产品。

华为云区块链服务是一种开放易用、灵活高效的通用型基础技术，聚焦于区块链云技术平台建设，帮助企业在华为云上快速、高效的搭建企业级区块链行业方案和应用，共同推动区块链应用场景落地，打造基于区块链的公共信任基础设施和共赢生态。

华为云区块链服务基于可信、开放、服务全球的华为云上运行，华为云产品和服务具有华为独有的新技术，以降低成本、弹性灵活、电信级安全、高效自助管理等优势惠及用户，BCS 可以和华为云技术产品和行业解决方案无缝对接，帮助企业在安全、高效、不可篡改等基础上轻松跨入云时代，快速部署新解决方案和应用。

5.1.1 区块链服务 BCS 的设计原则和产品定位

设计原则

- **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。BCS 能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，让客户简单使用区块链系统，专注于上层应用的创新和开发。

- **成熟先进**

BCS 在 Hyperledger、Kubernetes 和 Docker 等开源组件的基础上搭建，为用户提供成熟先进的区块链系统，华为云区块链服务秉承源于开源、优于开源、回馈开源的原则，积极投入和引领了多个开源社区的工作。

- **安全可靠**

  华为云区块链服务在开源的基础上注重自主创新，目前在关键领域如共识算法、同态加密、零知识证明、电信级云安全，高速网络连接、海量存储等方面具有自主知识产权的专利和技术积累。BCS 是在华为云完善的用户、秘钥、权限管理、隔离处理、可靠的网络安全基础能力和运营安全基础上推出的区块链服务。

- **云链结合**

  区块链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，华为云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，BCS 和华为云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**

  华为云专注于区块链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，共同打造基于华为区块链服务的可信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。

产品定位

华为云区块链服务致力于将自身技术使能企业的创新成长，面向企业及开发者提供一站式规划、采购、配置、开发、上线和运维的区块链平台服务，企业在华为云区块链服务上可快速自主搭建一套基于企业自身业务高安全、高可靠、高性能的企业级区块链系统，同时结合云服务特色的按需付费、弹性伸缩和可视化的数据管理等特性，大幅提高用户使用区块链的效率，有效降低企业的初始成本和使用成本。

5.1.2 区块链服务 BCS 的总体逻辑架构

在设计原则的指导下，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，华为云区块链采用分层架构设计、云链结合、优化共识算法、容器、微服务架构与可伸缩的分布式云存储技术等创新技术方案。

华为云区块链服务包括 4 层 2 列：

- **区块链资源层**

  华为云 IaaS 和 PaaS 层，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。

- **区块链服务平台**

  具有极强的可靠性和扩展性，后续根据市场需求逐步支持 Corda 和 EEA 等优秀区块链框架，为上层应用低成本、快速的提供高安全、高可靠、高性能的企业级区块链系统。

- **合约层**

  目前提供 Hyperledger 标准智能合约接口，用户可以根据不同应用场景构建不同的智能合约，后续将与合作伙伴一起为用户打造通用场景智能合约库，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场景。

- **业务应用层**

  为最终用户提供可信、安全、快捷的区块链应用。用户可以使用华为云提供的各种解决方案（例如供应链金融解决方案、游戏行业解决方案、供应链溯源解决方案、新能源行业解决方案等），结合合约层快速搭建区块链应用。

- **区块链系统安全**

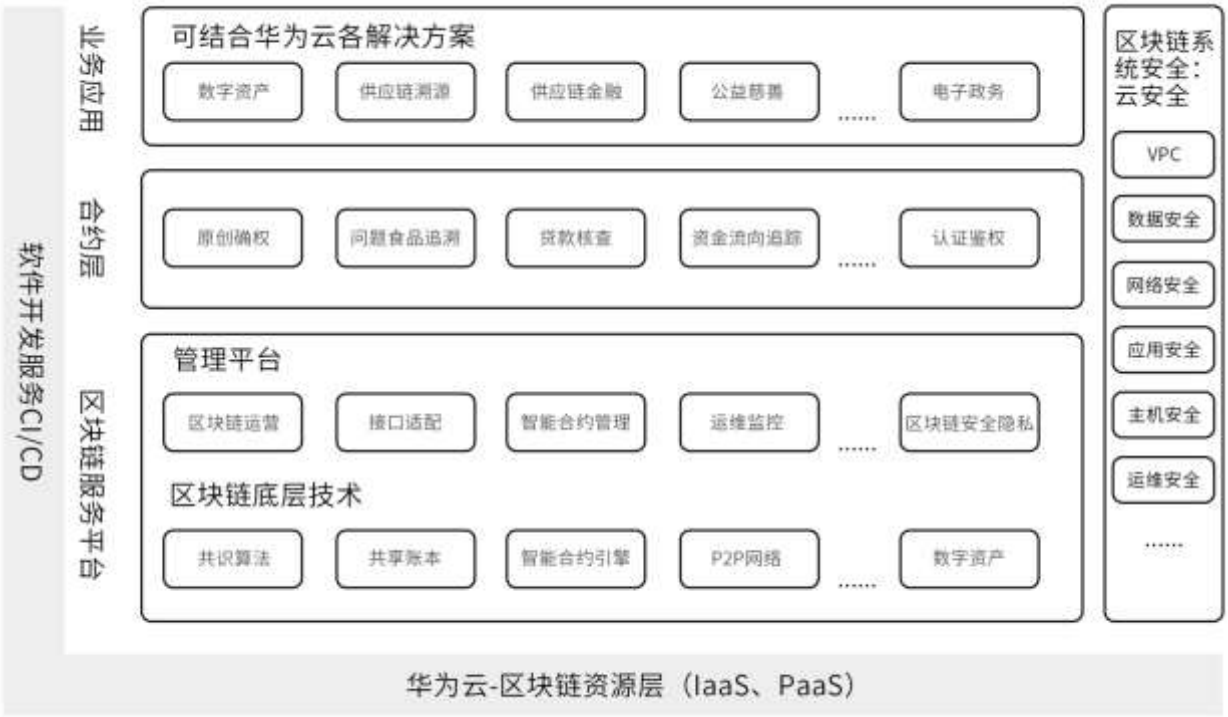
  由华为云安全提供，联盟链最重要的特点是节点的可控性和账本的安全，华为云安全可以为区块链节点、账本、智能合约以及上层应用提供全方位的安全保障。

- **软件开发服务**

  用户可以使用软件开发服务实现业务应用、智能合约从开发、测试到部署等 CI/CD(Continuous Integration/Delivery)全系列流程。

华为云区块链服务的分层架构设计有利于帮助企业快速简单的落地区块链场景，具体架构图如下图：

图5-1 华为云区块链服务逻辑架构图



5.1.3 区块链服务 BCS 平台功能特性

区块链服务平台是华为云区块链服务的主体，包括区块链服务管理平台和区块链底层技术两部分。

区块链服务管理平台

为企业提供快速创建、部署区块链应用、链代码管理和监控等全系统区块链服务。具体如下：

图5-2 华为云区块链生命周期管理图

通过设计以下模块来实现区块链系统全生命周期管理：

- **区块链服务运营模块**
  - 区块链服务配置

    BCS 提供的区块链配置页面简单易用，仅需配置几个参数如：区块链服务名称、部署区块链服务的 Kubernetes 集群名称，弹性文件名称、共识算法类型、节点参数等即可完成区块链服务部署。

  - 区块链服务部署

    配置完区块链服务参数后，租户点击确认按钮，一键完成区块链服务部署工作，PaaS 平台将根据用户配置的区块链服务参数和内置最佳实践通过 Kubernetes 将区块链的各个节点以 Docker 容器运行方式自动部署到指定集群中，相对于自建区块链系统，通过 BCS 只需要五分钟就可以部署一个完整的企业级区块链系统

  - 区块链服务状态监控

    通过区块链服务列表可以查看到区块链服务里节点的类型、数量和状态。方便管理员实时了解个区块链服务的状况。

  - 区块链服务节点管理

管理员可以根据业务需求和负载，按需购买资源，在运行时动态弹性调整 Peer 节点和 Orderer 节点的数目，可以有效降低企业的初始和运行成本，同时当节点出现故障时，系统对故障节点进行自动恢复，保障区块链应用的可靠性。

- 区块链服务联盟成员管理

华为云区块链服务提供联盟链方式，每个联盟成员为华为云独立租户，独立管理自己的节点和账本，BCS 通过独有的租户成员邀请机制，联盟发起成员可以通过租户账号邀请的方式将其他华为云租户加入到现有的区块链系统中，根据业务需求逐步扩大联盟链成员。后期根据市场需求将增加通过共识算法实现的节点成员自动加入机制，实现更加动态的成员管理方式。

- **区块链服务智能合约管理**

智能合约也称链代码（Chaincode），链代码将业务网络交易封装在代码中，最终在一个 Docker 容器内运行。租户可以在华为软件开发服务或者线下进行开发和测试。目前华为云区块链服务支持 Golang 语言编写代码，后续会推出 Java 等多语言支持，租户可以选择擅长的语言编写链代码。

a. 智能合约安装和实例化

链代码首先需上传安装在 Peer 节点上，然后在通道上进行实例化，实例化的过程需要参与方进行共识，智能合约实例化过程将被记录到区块链中，实例化后，链代码将在 Docker 容器中运行。

所有通道成员都需要在运行此链代码的每个 Peer 节点上安装链代码，且只需在一个 Peer 节点上进行链代码实例化。如需使用相同的链代码，通道成员必须在链代码安装期间为链代码提供相同的名称和版本。

b. 智能合约触发

智能合约实例化后，可以通过外部条件来触发合约执行的过程，支持定时触发、事件触发、交易触发和其他合约触发的方式。定时触发是指满足合约中预设的时间之后，节点就触发时间达成共识之后，自动触发合约调用的过程。事件、交易和其他合约调用都是在一次新的请求共识过程中触发合约执行。

c. 智能合约更改和清理

等合约条款需要变更时需参与方对新的合约共同签署后执行合约升级，或者对过期作废或者业务需求变更不再需要的合约进行转存和清理，升级和清理的过程需要多节点共识之后才能完成。

运维监控

为了租户能够快速准确地识别系统的运行状态以及在运行中满足其他的运维需求(如程序升级等)，华为区块链服务提供了完整、快捷、可视化的运维监控系统，包括监控、告警等功能。

- **监控**

  负责收集系统中运行的状态数据，并且可视化的呈现出来。系统中的状态数据包括系统的访问量、耗时、节点的健康状态以及比较底层的机器资源（CPU、内存、硬盘）使用状况等，通过可视化监控可以实时了解整个区块链系统的状态。

- **告警**

  对系统中比较严重的情况如欺诈节点、账本篡改、机器故障等情况通过邮件等方式通知到相关人员，以便及时处理。

区块链底层技术

- **共识算法**

  共识机制按照共识的过程分两类，第一类是概率一致的共识、工程学上最终确认；第二类是绝对一致之后再共识，共识即确认。华为云区块链服务定位为面向企业提供区块链服务因此采用第二类的共识机制，BCS 提供多种安全、高效共识算法，用户可以根据不同的使用场景以及安全和性能等不同需求选择合适的共识算法：

  - SOLO 模式：只需要一个共识节点，简单、快速，建议在开发测试环节使用。
  - 基于 Kafka/Zookeeper 高速共识算法：总节点数没有特定要求，能容忍半数以下节点发生故障。
  - FBFT 快速拜占庭容错算法：使用 3f+1 个节点，能容忍最多 1/3 拜占庭错误节点。

  详细对比见下图（f：fault）：

表5-1 共识算法参数对比图

共识算法	SOLO	Kafka（f 故障错误）	FBFT（f 拜占庭错误）
节点数	1	2f+1	3f+1
错误节点容忍	不容忍	最多 1/2 个 crash 节点	最多 1/3 个拜占庭错误节点
交易性能	一般	10000+TPS	2000+TPS

- **共享账本**

  包括区块账本、状态账本和历史账本三种账本：

  - 区块账本：记录智能合约的交易记录，保存在文件中。
  - 状态账本：保存智能合约数据的最新状态，保存在 KV(Key-Value)数据库中。
  - 历史账本：保存所有智能合约执行交易的历史记录索引，保存在 KV 数据库中。

- **持久存储**

  华为区块链服务将共享账本存在华为云弹性文件服务（Scalable File Service），SFS 为用户的弹性云服务器（ECS）提供一个完全托管的共享文件存储环境，符合标准文件协议（NFS），能够弹性伸缩至 PB 规模，具备可扩展的性能，为海量数据、高带宽型应用提供有力支持。

- **P2P 网络**

  网络中的节点之间通过 Gossip 协议来进行状态同步和数据分发。Gossip 协议是 P2P 领域的常见协议，用于进行网络内多个节点之间的数据分发或信息交换。其设计简单，容易实现，同时容错性较高。

- **智能合约引擎**

  运行在隔离安全 Docker 容器中，华为区块链服务实时监控智能合约在运行时是否存在高危函数调用和容器逃逸行为，预防恶意智能合约对区块链系统的威胁。

- **区块链安全隐私**

  华为云区块链服务高度重视区块链安全和隐私，除了华为云安全和 Hyperledger 自有安全措施外，BCS 还支持如下安全和隐私措施：

  - 支持国密算法和企业用户签名策略多样性：支持 SM2/SM3/SM4，使用基于硬件的可信计算环境保护秘钥安全性，效果较同样支持国密算法的同类产品有较大提升；
  - 加法同态加密：保护交易数据的隐私。
  - 零知识证明：保护交易参与方的隐私。
  - 为每个租户提供完整的 CA 证书管理体系，确保用户通过 PKI 证书体系保障交易身份认证、数据传输安全和交易内容隐私保护等需求。

- **接口适配**

  目前支持业务应用通过 Fabric 原生 SDK 调用智能合约，后续为了方便用户快速接入区块链系统，将提供 SQL API 和 Restful API 的方式接入，用户可以在 SDK、SQL API 和 Restful API 之间选择适合的方式调用智能合约接入区块链系统。

5.1.4 区块链服务 BCS 系统安全保障

联盟链相对于公有链一个非常重要的特点就是节点准入控制与国家安全标准支持，确保认证准入、制定监管规则符合监管要求，在可信安全的基础上提高交易速度才是有价值的。华为云区块链服务在云安全的基础上为区块链服务提供高安全环境。主要通过以下几个方面来提供安全保障：

- **安全可信的云平台：安全合规与标准遵从**

  20+全球权威认证，并持续增加满足全球不同区域与行业合规需求，主要包括中国公安部信息安全等级保护三级，可信云，金牌运维，CSA STAR 金牌认证，CSA C-STAR 和 PCI-DSS 等。确保云平台安全合规和标准遵从。

- **身份认证和访问控制**

  对公有云租户中的区块链服务用户，租户的访问控制能力是通过统一身份认证服务（IAM －Identity and Access Management）提供的。IAM 是面向企业租户的安全管理服务。通过 IAM，租户可以集中管理用户、安全凭证（例如访问密钥），以及控制用户管

理权限和用户可访问的云资源权限。使用 IAM，租户管理员可以管理用户账号（比如员工、系统或应用程序），并且可以控制这些用户账号对租户名下资源具有的操作权限。当租户企业存在多用户协同操作资源时，使用 IAM 可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安全，从而降低租户的企业信息安全风险。

- **区块链服务租户数据隔离**

华为云对云端数据的隔离是通过虚拟私有云（VPC － Virtual Private Cloud）实施，它将不同租户间的网络深度隔离，保证了不同租户间的数据不会被越权获取。通过 VPC，租户可以完全掌控自己的虚拟网络，实现不同租户间在二、三层网络的完全隔离：一方面，结合 VPN 或云专线，将 VPC 与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用 VPC 的安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离。在华为云区块链服务中区块链联盟成员独立为单独的一个租户，每个租户单独运行在一个 VPC 中，利用华为云 VPC 数据隔离机制来保障每个联盟成员的数据隔离和权限隔离，从而满足区块链系统的多中心化，多方参与，多方共识和不可篡改等独立、安全原则。

- **区块链服务账本存储安全**

华为云区块链服务将租户的账本存储的云弹性文件存储系统中在确保弹性扩展的基础上通过一系列的安全措施保障账本的安全。

- 密钥保护与管理

云弹性文件存储系统对接密钥管理服务 KMS（Key Management Service），KMS 是一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥安全，它通过使用硬件安全模块 HSM（Hardware Security Module），为租户创建和管理密钥，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露，保护密钥安全。KMS 对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，满足审计和合规性要求。

- 数据机密性保证

用户主密钥 CMK（Customer Master Key）由 KMS 生成、管理和销毁。华为云提供整卷加密功能。

- 可靠性保证

三副本备份，数据持久性高达 99.99995%。通过 VBS（Volume Backup Service） 实现云硬盘的备份与恢复，且支持通过弹性文件系统备份创建新的弹性文件系统。

- 数据删除与销毁

华为云致力于保护租户数据在删除过程中及删除后不至泄露，包括内存删除，数据安全（软）删除，磁盘数据删除，加密数据防泄漏和物理磁盘报废等。

- **华为云全栈防护体系**

以上几种安全措施是华为云安全为区块链服务提供的最重要安全措施，华为云还为区块链平台提供全栈防护体系包括不限于：网络安全，DDOS 攻击防护，应用安全（WAF 等，安全扫描），虚拟机安全，容器安全，数据安全和运营安全等等。通过华为云全栈防护体系可以确保用户的区块链系统免受各种安全威胁。

5.1.5 区块链服务 BCS 的技术特色和优势

在安全、可靠和高性能的华为云平台的基础上，根据“简单易用、成熟可靠、云链结合”等设计原则设计出来华为云区块链服务独特的架构，能为企业和开发者提供企业级区块链服务，具备以下几个方面的技术特色和优势：

高性价比

- **一站式开发、测试**

通过华为软件开发服务可以快速开发、测试和部署区块链业务应用和智能合约代码，为用户简化 CI/CD 流程，降低用户开发和集成成本。DevCloud 是集华为研发实践、前沿研发理念、先进研发工具为一体的研发云平台；面向开发者提供研发工具服务，让软件开发简单高效。

- **一键上链**

让企业和开发者最快 5 分钟完成企业级商用区块链服务的部署和运行，相对自建区块链能节省 80%的开发和部署成本。

- **按需付费**

用户可以根据需求对使用的资源进行动态调整，根据需要付费，能减少 60%的初始成本和运行使用成本。

- **全程运维和监控管理**

BCS 和华为云平台，为区块链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。

高性能

- **高效接入**

华为云具备电信的高速网络通信能力，和高并发、快速接入的能力，能最大可能的满足用户对区块链高效接入的需求。

- **高性能共识**

BCS 为用户提供多种高效共识算法（SOLO，基于 Kafka 的 CFT 故障错误容忍，FBFT），FBFT 是对拜占庭容错共识算法进行深度优化，在安全和效率达到最佳平衡点。用户可以在 2000+TPS 和 10000+TPS 共识算法上根据业务需求和场景进行选择。

- **秒级共识**

用户可以根据业务需求将交易速度设置到到秒级甚至更低，满足业务性能需求

- **高效的存储速度**

BCS 将区块链账本存储到华为云高效弹性存储文件中，能最大程度满足用户海量快速存储需求，根据市场需求逐步推出区块数据存储到关系型数据库的能力，从不同角度满足用户对存储速度的要求。

高安全

区块链业务存在以下安全需求：

- 联盟链的特点：节点、账本的可控制，满足监管和准入需求。

- 通过分布式账本实现不可篡改的加密交易数据。
- 交易可追溯不可抵赖。
- 隐私保护：交易匿名，交易不可关联。
- 可监管和审计。

华为 BCS 通过三种途径保护区块链安全：

- 使用华为云安全保护区块链系统可靠运行。
- 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、隐私保护的能力。
- BCS 在此基础上对高安全要求用户提供更进一步的安全隐私保护，如通过硬件保护密钥，同态加密和零知识证明等。

高可用

- **高可用架构**

  BCS 运行在高可用华为云上以及基于 Kubernetes 和 Docker 构建，具备快速拉起，节点和成员弹性伸缩能力以及节点故障自动恢复能力，从架构根本上保障区块链系统的高可用能力

- **高可用的接入和存储方式**

  提供原生 SDK、SQL-API 和 Restful API 三种智能合约调用方式，用户可以根据不同业务需求和使用习惯选择可用的接入方式。区块链账本使用云弹性存储系统进行存储，具备安全、弹性扩充、海量存储和自动备份的能力，实现存储的高可用。同时为区块提供文件存储和关系型数据库存储两种可选方式，用户也可以通过关系型数据库的高可用性来保障区块的稳定和可用。

- **提供全球部署和多种部署方式**

  华为云区块链服务将逐步实现在华为云不同管理域和全球合作云上部署的能力，逐步具备区块链全球部署能力，最大程度实现区块链的多中心化的能力，保障区块链系统的安全和高可用。华为云区块链服务实现联盟链和私有链的部署方式，能满足不同企业和用户对区块链系统的部署要求。

5.2 华为对区块链的整体构想

图5-3 华为区块链整体构想

华为区块链的整体构想是：聚焦典型应用领域，以区块链平台为核心，联合网络和可信硬件执行环境（终端+芯片），形成三位一体的端到端区块链框架，实现软件+硬件结合，提供更快、更安全的区块链端到端解决方案。

可信硬件执行环境：加强硬件能力，软硬结合，大幅提升区块链的安全性和性能

安全和性能是制约区块链网络发展的两个关键技术因素，所有的区块链都是在这两者之间寻求平衡。目前的技术主要是在共识算法和共识机制等软件层面进行提升，而未来通过可信硬件环境提供芯片层级的区块链安全和性能加速，是业界考虑的一个重要方向。

我们愿与各方产业伙伴一起，构建安全高效的区块链网络。

网络：网络要纳入到区块链中，成为区块链中重要一环

面对区块链未来发展，网络面临两个问题：

- 随着 hyperledger 等技术的改进，区块链的应用领域已经发生改变，支持的节点数也在不断增加。在当前 P2P 架构网络下小量节点的互联没有问题，但面对未来区块链的节点数的激增，对于上百节点的区块链，P2P 大面积的发送广播报文，将会对网络带宽产生极大的浪费。
- 区块链早期的设计是去中心化，以降低集中核心故障或存在数据不可信的影响。而随着联盟链的普遍使用，当初的去中心正在向多中心的方向进行发展，区块链仅解决分布式部署下，数据中心的账本一致性问题，而网络在承载中的可靠性尚未考虑。

华为认为网络设备要纳入区块链的链条，增强网内可靠性。伴随着边缘计算的普及，当前的网络设备已经部分具备一定的计算能力，依托网络边缘的计算能力，将网络设备纳入区块链，即保证了网络设备的安全性，同时将网络信息作为链上信息的一环，一方面缓解云平台的在大量节点下对计算和存储的压力，另一方面也对未来大量的 IoT 设备的合法接入进行认证管理。针对区块链设计网络演进是未来考虑的一个方向。

6 总结：华为对区块链未来发展判断

区块链是开放的数字价值的流转，其构建一种新型的价值网络，用技术为信任背书，对其未来的发展判断如下：

- 从应用维度上，2018 年是区块链的应用元年，在标准没有完善前，在不同行业的试用是重点，政府数据存证、IoT 领域物流和车联网的应用、运营商云网协同和供应链金融将进入首发试用阵容。本质上这些领域急需借助区块链构建公开透明的营商环境。
- 从技术维度上，安全是构建区块链需要考虑的重要问题，国密算法将会成为区块链在国内主要市场应用标准，区块链的框架将包含云，管，端三层，以软件+硬件相配合的方式，构建高度可靠的安全能力。
- 从区块链产业发展上看，中美欧会成为区块链应用的重要区域，区块链不会昙花一现，我们可以依靠区块链在技术竞争中占据先机，而这些需要明朗的产业政策给予保障，目前看到国内从中央到地方政府机构都在努力构建区块链的孵化环境，推动区块链产业健康发展。这就为我们发展区块链技术和产业创造了良好环境。

基于以上判断，为有效推动区块链产业的快速发展，实现建立可信社会的目标，有如下建议：

- **依托联盟，形成产业合作，加速我国区块链标准快速落地**

  区块链技术尚未成熟，从国内外的标准推动来看，区块链标准在 2017 年有推进但速度较慢，这极大影响了区块链的产业节奏；同时安全一直是区块链技术的核心，但涉及到算法，系统等的标准问题仍然存在。因此，建议以国家机构牵头，借助产业的力

量，通过联盟加速区块链标准的制定，特别是跨链、加密算法等重点标准在国内的落地，占领区块链产业在国际上的话语权。

- **构建区块链产业孵化环境，推动区块链产业发展**

  鼓励从企业到政府的区块链应用试点，在国内建立区块链的应用孵化环境，在应用中发现问题，逐步推进。现在有些区块链项目说的多，做的少，以炒概念而获得投资为目标，这对整个区块链产业的健康发展是不利的。因此，建议国家或重点企业积极进行试点，推动区块链应用孵化，优化产业环境，加速产业成熟，在新一轮的区块链市场竞争中获得先机。

- **清晰化区块链技术和应用的产业政策**

  目前我国的区块链产业政策由各部门和部分省市分别进行小范围的推广，结合我国在互联网+的发展思路，政府需要明确清晰的区块链产业政策，展开对区块链技术的支持、标准的推进、区块链方案的研发、示范性工程的建立等等一系列行动。特别是对区块链应用的监管和放权并举，推动区块链技术和应用在市场中良性发展。

- **积极参与开源社区，倡导企业间区块链技术的互通交流**

  鼓励在参加国际区块链开源社区，快速完善区块链能力的同时，加强国内企业间的合作，对区块链技术进行攻关、方案研讨、技术贡献等，聚拢产业力量，提高国内企业在国际区块链技术竞争中的影响力，实现产业共赢。