Lenovo 联想

联想区块链技术白皮书

前言

区块链技术对于当今任何企业来说都是一项非常前沿的技术，在区块链业务上企业都会遇到来自于技术、人员、需求等不同层次的挑战。具体来说，这种不确定性主要有两个方面：

- 区块链技术平台还处于发展早期，尚未形成业界一致的平台和技术标准；
- 区块链技术如何与现在业务的结合，并有效的将场景落地仍在探索中。

为了能够快速应对这些挑战，联想在区块链项目的推进方面有以下四大亮点：

- 在实际应用落地方面，联想从供应链选取了几个具体案例，进行小规模敏捷开发，迅速实现场景落地，并逐渐将经验开放至其他业务领域。
- 在组织管理方面，联想内部组建了跨组织的 LeChain 团队，这是一支集研究、开发和运维一体化（DevOps）虚拟团队，成员来自数据中心集团的供应链战略部门（业务内部需求），BT&IT（需求商业化及开发）、研究院（技术攻坚），能够从市场洞察、内部管理、关键技术、平台开发等多个角度给出专业性意见，并能够就项目关键问题迅速形成共识。
- 在场景具体需求分析上，LeChain 团队引入创新设计思维（Design Thinking）思想，兼顾了技术（区块链）、业务（供应链），人（以人为先）的多方元素，运用头脑风暴推进挖掘更多的新商业场景，从而实现以客户为中心的各种应用和服务。
- 在具体场景以来的技术领域、联想集中力量突破技术瓶颈。例如在隐私保护上，联想实现了对身份、交易数据、智能合约、交易状态的四重保护；又如在对接现有 IT 系统上，联想提出了可跨越不同类型企业网络、可统一管理的解决方案。

联想在行业智能化变革上，始终提倡数据、计算力、算法三个要素相互依赖、缺一不可。而联想自身在上述三个领域有着强大的先发优势。作为智能制造领域的先锋和领军企业，跨必须啊办法结合了自身在硬件、软件，人工智能，大数据。物联网等领域的优势。积极推动区块链核心技术和平台的应用及开发，必将为新时代赋能，助力各行业迎接智能化革命的浪潮。

主要编撰人员：

联想 LeChain 项目组，其成员分别来自联想研究院、联想 BT&IT 和联想数据中心集团。具体名单如下：

联想数据中心集团供应链：Robert Bernard、郑懿、董洁容

联想 BT&IT：陈建彬、李京生、李月田、牛海保、孙阳秋、张桂平

联想研究院：王云浩、陈飞飞、谭崇康、李春燕、郭青霄、汤文军、杨立中、黎丁豪、马逸龙、过晓冰

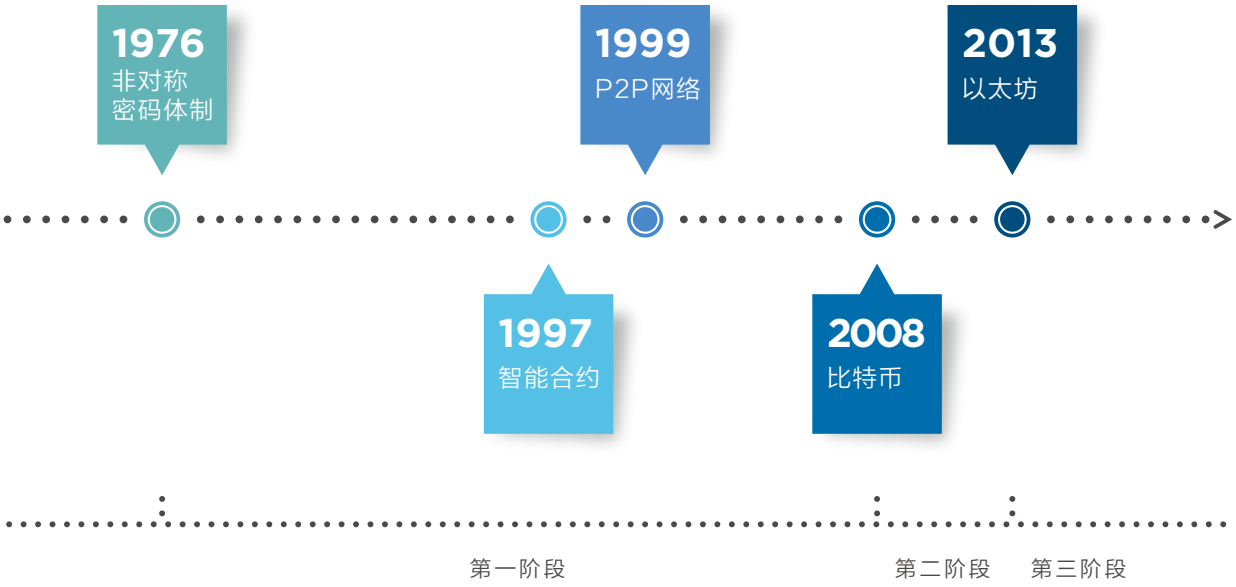
目录 CONTENTS

1 区块链简介

区块链技术作为新一代信息技术的代表之一，与人工智能、量子信息等信息技术一同加速突破应用，使全球进入科技创新空前密集活跃时期。区块链技术因具有去中心化、不可篡改、可追溯等特征吸引了政府部门、金融机构、科技企业、资本市场等投身其中。我国区块链产业已处于高速发展阶段，越来越多的创业者和资本不断涌入，企业数量急剧增加，未来必将重构创新版图、重塑经济结构[1]。

区块链的发展历程

区块链技术的应用始于比特币。比特币将传统中心化网络中可信任的单一个体（例如银行）转变为非中心化网络中多个个体，这一过程彻底摆脱了对银行等金融机构信任背书的依赖，这也正是区块链技术的核心——去中心化，即去除所有信用中介。区块链技术发展至今可分为三个阶段，如图 1-1:



图：区块链发展历程

01 第一阶段（~2007 年）：区块链底层技术发展阶段

1976 年，W.Diffie 和 E.Hellman 两位密码学家在发表的《New Direction in Cryptography》（中文译名：密码学新方向）[2] 的论文中，提出了“非对称加密体制（公开密钥密码体制）”的概念，开创了密码学研究的新方向，为此后的 RSA 算法、椭圆曲线密码学（Elliptic curve cryptography，ECC）等密码学算法的诞生奠定了基础。1980 年，Merkle Ralf 提出了默克尔树（Merkle tree）数据结构以及相应算法，该算法主要应用于分布式网络中数据同步正确性校验。1982 年，Lamport 提出拜占廷将军问题（Byzantine failures），标志着分布式计算的可靠性理论和实践进入到了实质性阶段。1997 年，Adam Back 提出了 HashCash 方法，这被认为是第一代工作量证明算法（PoW, Proof of Work），以及差不多同期提出的 P2P 网络（Peer to Peer），这些都为随后比特币的问世起到至关重要的作用。

02 第二阶段（2008 年 -2012 年）：区块链 1.0 阶段

2008年11月中本聪（Satoshi Nakamoto）发表的《Bitcoin:A Peer-to-Peer Electronic Cash System》（中文译名：比特币：一种点对点的电子现金系统）[3]标志着区块链进入1.0阶段，该阶段的主要特征是可编程数字加密货币体系。区块链技术是比特币（Bitcoin）的底层技术，是一个去中心化的共享总账，采用密码学的方式保证了账本的不可篡改性和可追溯性。区块链1.0阶段的不足在于智能合约系统不完善，导致其应用在非金融场景十分困难。而且其架构设计不够灵活，每个区块的大小只有固定的约1M左右，能够记录的信息非常有限；此外性能也非常低下，据测算其每秒钟平均支持约7.3笔交易；上述问题都极大地限制了其使用场景和应用范围。

03 第三阶段（2013 年 - 至今）：区块链 2.0 阶段

2013 年以太坊（Ethereum）的出现首次完整支持了智能合约，业界比较公认此时区块链技术进入 2.0 阶段，该阶段的主要特征是可编程智能合约系统。以太坊在比特币的基础上进行了重大改进，完善了脚本系统，支持包括 Solidity 在内的高级语言使合约能够应用在各种金融领域甚至非金融领域，且实现了更加精细的账目控制，同时，对应的底层协议非常简单。从这个意义上讲，比特币区块链网络本质上是一套分布式数据库，而以太坊可以被看作是一台分布式计算机系统。比特币和以太坊是典型的公有链，任何人均可随时参与、退出。加入到网络中的参与者可以匿名互动，当然，这样的场景并不能满足企业级应用的需求。2015 年 12 月，针对企业级需求，Linux 基金会（Linux Foundation）宣布创建超级账本开源项目 Hyperledger，一共有 30 家企业成为发起成员，该项目的创始成员于 2016 年 2 月公布，另有十名成员和理事会的组成在 3 月公布。2016 年初，超级账本推出了 Fabric 子项目。Fabric 主要基于 Digital Asset 和 Blockstream 的 libconsensus 以及 IBM 的 OpenBlockchain，具有高度模块化和可配置的体系结构，为包括银行、金融、保险、医疗、人力资源、供应链甚至数字音乐交付在内的广泛行业用例提供了创新、多功能性和优化。超级账本的最大优势在于架构的灵活性，其模块化设计使得各种底层组件均支持可插拔可替换，包括共识协议等。这样，使得超级账本平台能够更有效地为不同商业环境定制，以适应特定的场景用例和信任模型。除了 Fabric 子项目，后期也有更多的公司在超级账本中创建子项目并贡献代码，例如以 Intel 公司为主导的锯齿湖项目（Sawtooth Lake）等。2016 年 11 月 30 日，R3 的基础设施 Corda 项目宣布开源。Corda 被设计为一个分布式账本，用于金融机构之间，还可以限制各方能够看到什么类型的信息。Corda 实质是一个去中心化的数据库，甚至还预留了 SQL 接口。这个数据库受到多交易主体之间的业务关系约束的。Corda 被认为是“有链无块”的区块链技术，其原理是让后续交易直接指向前序交易，以实现数据不可篡改和可追溯的特性。

区块链技术在飞速发展，各个应用领域的从业者们也开始探索并尝试使用区块链技术。而对于其下一阶段的发展或者说何时进入区块链 3.0 阶段，业界存在较大争议。有专家主张区块链广泛应用才是 3.0 的标志，也有支持区块链和其他主流技术融合后成为 3.0 主要标志，例如 “区块链 + 云计算”、“区块链 + 物联网”、“区块链 + 人工智能”等。但区块链作为一项颠覆性技术，正在引领全球新一轮技术变革和产业变革，推动着“信息互联网”向“价值互联网”变迁，这点已经毋庸置疑。

区块链的关键技术

区块链技术是分布式账本技术（DLT,Distributed Ledger Technology）的一种具体的技术实现形式。分布式账本技术是一种支持分布在多地点（跨组织、跨地域）的数据复制、共享、同步并达成共识的数据库技术。分布式账本技术根据对数据的组织和分类算法不同，有多种实现形式，其中区块链是目前发展的主流。

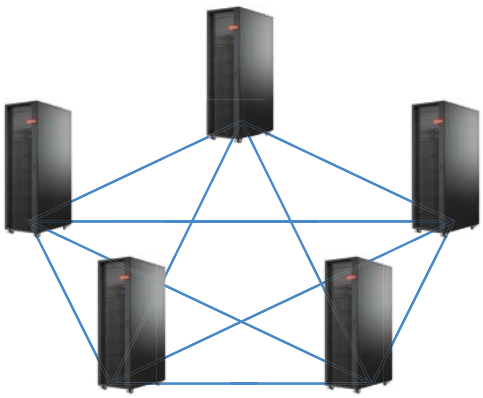
区块链的底层关键技术包括 Awarding（激励机制）、Blockchain（块链式存储）、Consensus（共识协议）和 Decentralization（去中心化架构），每个英文单词的首字母正好组成 BCD.，以下将逆序逐一介绍各技术要点。

去中心化架构（Decentralization）

区块链是一种分布式数据存储结构，没有中心节点，所有节点都保存全部的相同的区块信息，理想情况下是一种完全实现去中心化架构。对于特殊的应用场景，可以适当地采用弱中心化的管理节点，即中心节点不影响整个区块链结构的运行、或者说架构确保了中心节点可实时替换、对中心节点只是一种弱依赖关系；若从安全角度来说，弱中心化结构中的中心节点要满足对于区块链的安全不构成威胁，对用户隐私不构成威胁等。

去中心化架构的实现大体包括如下三种：

- 零中心，即无中心，节点完全对等。网络中的每一个节点都具有相同的权利和义务，如图：区块链去中心化 P2P 网络架构图。这是一种最理想的情况。
- 多中心或者弱中心化架构，这些中心节点对等，即在链上存在多个中心节点，还有其他非中心的普通节点，所有的交易必须通过这些对等中心节点进行处理，这种架构是兼顾性能的一种折中方案，比较典型的例子就是 EOS 网络。
- 中心轮换随机挑选，即每个节点均有担任中心节点的机会，且中心节点随机选出。借助这三种实现方式，区块链系统具备了容错性、抗攻击力和防合谋等优点。



图：区块链去中心化 P2P 网络架构图

随着区块链技术的发展，去中心化的架构还需要支持自组织特性，即当多个区块链网络相互对接时，怎么保证链内自治，链间协作，这也是目前的研究热点之一，例如多链和跨链技术。

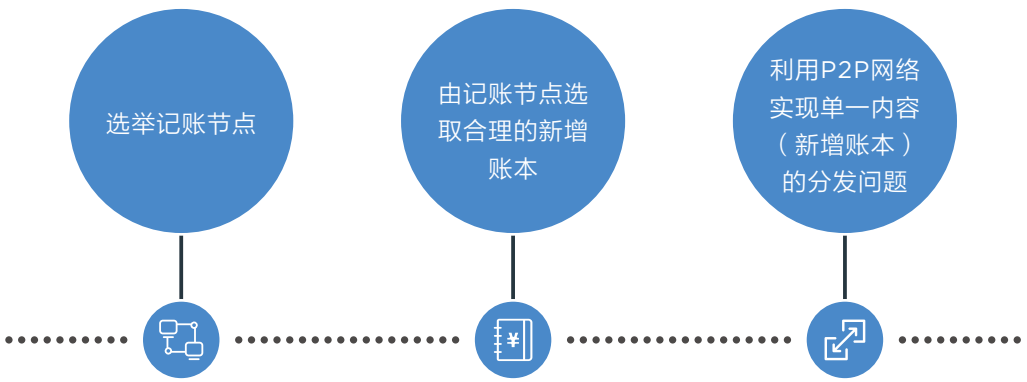
区块链中的“去中心化”不等于去监管，监管与“去中心化”并不冲突，“去中心化”去的是中央控制方，而并非监管方。由于区块链的公开透明特性，监管机构反而可以更加方便地监控整个系统的交易数据，而且由于区块链的防篡改特性，交易一旦发生后即不可更改、不可删除，那种完全依靠数据造假蒙蔽监管的情况反而就很难发生了，这显然更有益于监管机构对市场行为进行监督。

共识协议（Consensus）

在区块链网络中，采用共识协议或者共识机制的办法来保证去中心化的网络中各节点上账本的一致性。在共识的理解上，随着其范畴的不同而有着不同的定义，可以据此定义为大共识和小共识。并且，从共识本质上理解，智能合约其实也是共识的一部分。

大共识与小共识

所谓大共识，即广义共识，是指所有确保各节点上账本一致的协议规范和流程控制。从这个意义上讲，共识协议包括账本数据的一致性，网络传输的一致。其中，前者主要确保不同节点在记录账本时的一致性，具体包括，确保各节点的时间同步、统一记账内容并处理。在共识协议上，区块链针对较难解决的异地同时记账模式，借鉴了 P2P 在同一内容分发上的高效性。具体思路是先由单一节点集中记录并生成唯一的新增账本、再利用 P2P 网络统一分发的思想。基于此思路，因此，一个简单的共识协议包括：



在广义共识的定义步骤中，考虑到步骤 3 的实现过程相对而言比较标准，各共识协议主要是围绕记账节点选举上有着不同的实现方式，因此也常把记账节点的选举机制（以及新增账本的确定）作为共识协议的核心内容，这就是小共识的含义，或者说狭义共识协议的含义，即选举特定节点记录新增账本的机制，这机制在节点上的具体实现逻辑，也叫共识机制或共识算法。

超级账本 Fabric 的共识过程与之类似，只是省去了选举记账节点的过程，其基本思路是：预先审核新增交易真伪并排序，然后按时间顺序对新增交易打包并利用 P2P 网络（例如 Gossip[4]）实现分发。

表 1-1 典型分布式账本共识算法分类及其优缺点

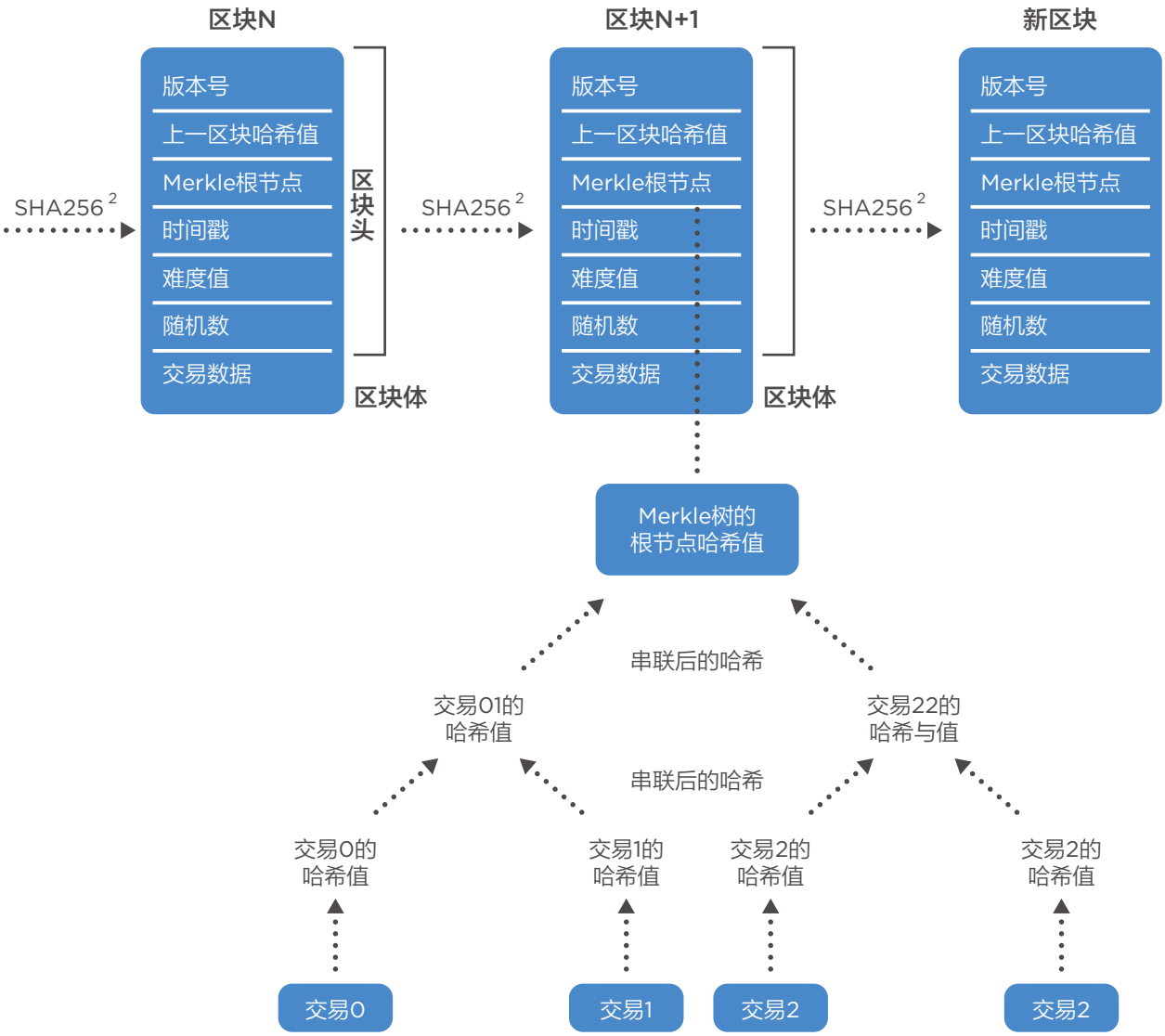
分类	基本原理	优点	缺点
PoW （Proof of Work）	通过大量运算，第一个计算出一个满足规则的随机数，即获得本轮次的记账权，由其发布新增账本，全网其他节点验证后一起存储。	易于实现，选举机制与算力成正比，节点间无需交换额外的信息即可达成共识，恶意破坏账本体系需投入极大的成本。	浪费计算资源，区块链确认时间长，因此共识达成周期长，效率低。
PoS （Proof of Stake）	记账权与权益成正比，而不是和算力成正比。主要是在计算随机数的时候，其计算难度和每个节点所持权益的时间占比成反比，这样对于权益高的节点，其计算难度非常小，更容易抢夺记账权。	解决 PoW 消耗算力的问题，在一定程度上缩短了共识达成的时间。	机制略复杂，计算资源仍有一定程度的浪费。
DPoS （Delegated Proof of Stake）	类似于董事会投票，由权益拥有者投票选出一定数量的节点，并由这些选举产生的节点，代理它们进行验证和记账。具体记账权由这些被选出的节点，按一定规则来依次记账（例如，按照时间片轮流的方式）。	大幅度缩小参与验证和记账节点的数量，理论上可以实现秒级的交易确认。	机制较复杂，而且真正参与记账节点数较少，因此安全性鲁棒性都有所下降。
分布式一致性算法	分布式一致性算法是基于传统的分布式一致性技术，包括解决拜占庭将军问题的拜占庭容错算法（BFT: Byzantine Fault Tolerance）和解决非拜占庭问题的分布式一致性算法（Paxos、Raft）。	实现秒级的快速共识机制，保证一致性。	网络规模不宜太大，更适合多方参与的多中心商业模式。

智能合约

智能合约就其本质而言，也是一种共识的概念。值得注意的是上述的共识机制，都是针对已经发生的交易，进行记录并同步到所有节点。而智能合约究其目的，是确保未发生的交易，在条件满足后能自动触发并生成新的交易，并且这些未来的新交易能保证在各节点上记录的一致性。从这个意义上讲，智能合约是对未来交易的共识。具体而言，智能合约的技术包括合约的签署和分发，合约条件的触发以及最终的记录入链等。

块链式存储（Blockchain）

块链式存储，是指区块链的数据组织方式。区块链采用了块状（Block）数据结构，以块为最小单位，并且块间采用了链式（Chain）数据组织方式。数据打包成块，每个块通过特定的信息链接到上一个区块的后面，形成一套完整的账本，并在区块链网络中存储该账本。Blockchain 正是区块链名称的由来。块链式存储，较之传统的表式（table）数据库而言，更适合累加方式记录数据，容易实现数据的不可篡改和可追溯。



图：比特币数据结构图

区块链中区块结构包括区块头和区块体两部分，区块结构如图：比特币数据结构图。区块头中包括：随机数、时间戳、难度系数、前一个区块的安全散列值（SHA,secure hash algorithm 安全散列函数计算的结果，即上一个区块的默克尔树根）、当前区块全部交易对应的默克尔树根。随机数是记账节点在抢夺记账权时计算出的结果；时间戳表示区块结构生成的时间，区块链结构中，前一个区块的时间戳会比后一个区块的时间戳小，能够保证区块链有序地形成，也具有防篡改的作用；难度系数是节点计算数学难题的难易程度，可以人为进行调整，从而实现了对出区块速度的控制；默克尔树根为对当前块内全部交易进行安全散列函数运算得到的，由于交易不相同，所以每个区块的默克尔树根都不同，默克尔树根确保了记录的交易不被篡改。最终的链式，是通过区块头中存储前一个区块的默克尔树根和后一个区块的默克尔树根连接而成。在具体的出块过程中，把从创世区块开始到当前区块的长度称为高度（Height），而且区块链网络中，从创世区块到高度最高的块对应的链式结构称为主链。节点在抢夺记账权形成区块链的过程中，会因为网络的延时或其他情况而导致区块链分叉，针对分叉情况，可以根据预先设定的规则让其余节点自动选择并保留对应的区块而放弃其他分支，例如选择高度最高的，相同高度的时候选择难度最大的，相同难度适合选择安全散列结果最小的等等。区块链技术运用非对称加密算法和安全散列函数实现区块链中交易的数据加密过程和签名过程。上述技术最终确保了交易数据的无法乱序、无法撤销、无法仿冒、无法篡改等特性。

随着技术的发展，区块链的数据结构也在不断演化，最近的一些新的尝试，提出基于 DAG（有向无环图 Directed acyclic graph）[5][6] 等数据结构来取代块链式存储，以提升其交易并发时的写性能，相关实现包括 IOTA[7]、Byteball[8] 等。

激励机制（Awarding）

区块链系统的长期运转，需要设计一种鼓励参与者长期支持、共同维持的制度机制。激励机制的宗旨在于激励参与者能持续投入（甚至不断扩大投入），最终确保系统的稳定。而面对企业级应用，例如区块链应用于特定成员间的商业场景（即联盟链），自身其实不需要附带激励功能，因为各参与者的商业诉求可以预先设定，并据此明确区块链网络维护的职责，包括如何管理和维护区块链等。但区块链若应用于公共事务，就必须依赖激励机制，否则系统将无以为继。

比特币、以太币以及其他各种虚拟货币 / 代币（token），正是区块链具备激励功能的体现。在比特币中，网络中的每个节点不断通过抢夺记账权（通常称为“挖矿”，其实质为 1.2.3 中提及的计算满足某个难度的随机数的过程）来创建新的区块，共同维护区块链的延展存续，获得记账权的同时将得到相应的“报酬”（数字货币）。比特币中的激励机制之所以能够有效地维护区块链网络中的账本，原因在于成功抢夺记账权后的巨大收益，确保有大量节点愿意投入算力来参与，从而客观上维护了网络的稳定性。若有恶意节点想要破坏区块链网络中的账本，其所付出的代价是非常大的。

区块链发展至今大致分为公链、联盟链和私有链。以太坊是公链的典型应用场景，它的激励机制是 gas 系统。gas 是衡量执行账本操作所需的计算量的单位，用来表征为执行操作而需要支付给网络的费用数额。以太坊对智能合约的操作都需要一定量的 gas 来支付。与之对应的是联盟链和私有链，其典型应用是超级账本 Hyperledger Fabric。原生的联盟链或者私有链都不依赖激励机制，因此其不支持代币（token）机制，但我们也看到，最新的一些研究已经基于 Hyperledger Fabric 实现了对代币的支持，包括 IBM[9]、纸贵科技 [10] 等。上述实现虽然开始支持 token，但其目的和本节阐述的激励有差别，因为对代币的支持其实与节点对网络的贡献度无关，即节点参与账本的维护，不影响代币的分配和再分配。具体的实现上，以 [9] 为例，针对区块链技术和智能合约的挑战提出 Fabric Token 生态系统的解决方案，该方案允许用户和企业轻松采用区块链技术和智能合约，并将包含四个主要组件：第一个组件是 Fabric Token 本身，它将用作支付生态系统内产品和服务的功能实用程序。第二个是 TokenGen，一个用户友好的平台，用于为令牌经济生成智能合约。第三个是 DApp Workbench，一个一体化的解决方案，适用于希望将区块链技术和智能合同集成到业务流程管理中的企业。最后一个组件将是 Fabric Store，这是智能合约组件的分散市场，这将允许第三方开发人员进一步扩展 Fabric Token 生态系统的功能范围。

区块链的理解误区

区块链的快速发展，使得很多理论还没有取得业界一致的看法，甚至包括对某些基础定义的理解，因此在媒体上能看到一些互相矛盾的理解，造成了理解的误区。

关于“伪链说”

关于区块链的实现机制，业界部分专家根据其对中心化服务的依赖程度，共识机制等，分成了真链、伪链和非链等类别[11]。1.2 的关键技术描述来看，区块链实质是一种分布式的数据系统，其采用包括非对称加密、安全散列函数等安全机制后，使得账本系统不可篡改，并且借助网络传输最终实现存储的一致性。从这个本质看，只要本身的数据系统已经是分布式存储，其存储机制符合不可篡改特性，并且数据的一致性是由共识算法和网络一致性得以保障，那就是区块链系统。

基于上述理解，一些所谓伪链，其实仍符合区块链的实质，例如超级账本的 Fabric 方案。有专家担心其全部交易信息都要经过 Zookeeper 软件处理，而 Zookeeper 存在中心化的实现，因此得出超级账本是一个中心化的系统。正如我们在 1.2.1 提到，弱中心化的系统，实质是架构确保了中心节点可实时替换、对中心节点只是一种弱依赖关系。显然，Zookeeper 软件本身在 Fabric 架构中其实较容易被替换，而且数据的生成、维护都不强依赖于该服务体系。甚至在 Fabric 网络中，通过合理的隐私保护增强就使得所有的辅助节点（包括排序节点、Zookeeper 等）屏蔽对用户数据的读取。因此仅凭存在中心化服务入口就断定 Fabric 是伪链的推理是不成立的。事实上，目前大部分互联网服务就目前实现而言，往往也是中心化的，比如 DNS 域名解析服务，这主要是为了节省成本并提高效率。但只要该服务不影响最终数据的生成、维护，我们仍可以认为其符合区块链定义。

关于 BaaS 云区块链平台

现在主流的 BaaS（Blockchain as a Service）平台，几乎都是基于云平台。甚至有专家认为，BaaS 的唯一实现方式就是基于云。相比传统的分布式物理机器的区块链实现，BaaS 云区块链平台实现了两大突破，首先基于虚拟机的管理，使得平台的管理和实现更为标准化，这样无论平台方还是实际使用客户都更为方便快捷，其次云也降低了用户的初始采购成本以及后期的管理维护成本。

事实上，云只是 BaaS 区块链服务的实现方式之一，并且是一种鲁棒性较差的实现。理想的云计算方案，其可靠性完全由云平台层提供并保障。因此纯云的 BaaS 平台是否真实存在多份拷贝、多个物理节点维护账本，其底层完全是不透明的。这样会削弱甚至破坏区块链的理念。极端情况下，用户可能得到的是一个完全“虚拟”区块链系统，这可能是另外一种形式的伪链。即尽管从用户视图看有着多份账本系统，但实质却都对应同一物理主机甚至同样一片存储区域。

从实质出发，区块链应该由实际不同系统、甚至由完全异构的主机组成的多机协同的网络系统，越多样化，则系统的鲁棒性越高。事实上，即使在云平台的方案中，也应该由不同品牌、不同位置的公有云来组建的，这样更符合区块链的理念。因此，在具体实现 BaaS 平台时，一个纯云的方案，尤其是高度虚拟化的方案，需要用户认真判断其实际对应的物理系统，是否真存在多份数据拷贝，这些数据的内容，是否真的跨地域、甚至跨异构系统。

区块链应用领域

区块链的商业价值

数据透明，增强信任

区块链技术具有数据不可篡改、交易可追溯以及分布式账本一致性，可以很好的解决商业流程中由于数据不透明引起的各种纠纷，并实现有效的追责和产品防伪。

商品来源以及各流通环节的不透明性是困扰消费者和企业的焦点问题。以食品为例，虽然有各种安全防伪标识，但是从源头到生产、到运输、到最终消费者整个链条中环节众多、流程冗长，消费者无法了解全面信息，难以判断最终的真实性，影响社会和企业的公信力。采用区块链技术后，全流程数据透明，各流通环节的真实信息可以任意追溯，从而打造一个良好的信任生态体系。

提升效率，降低成本

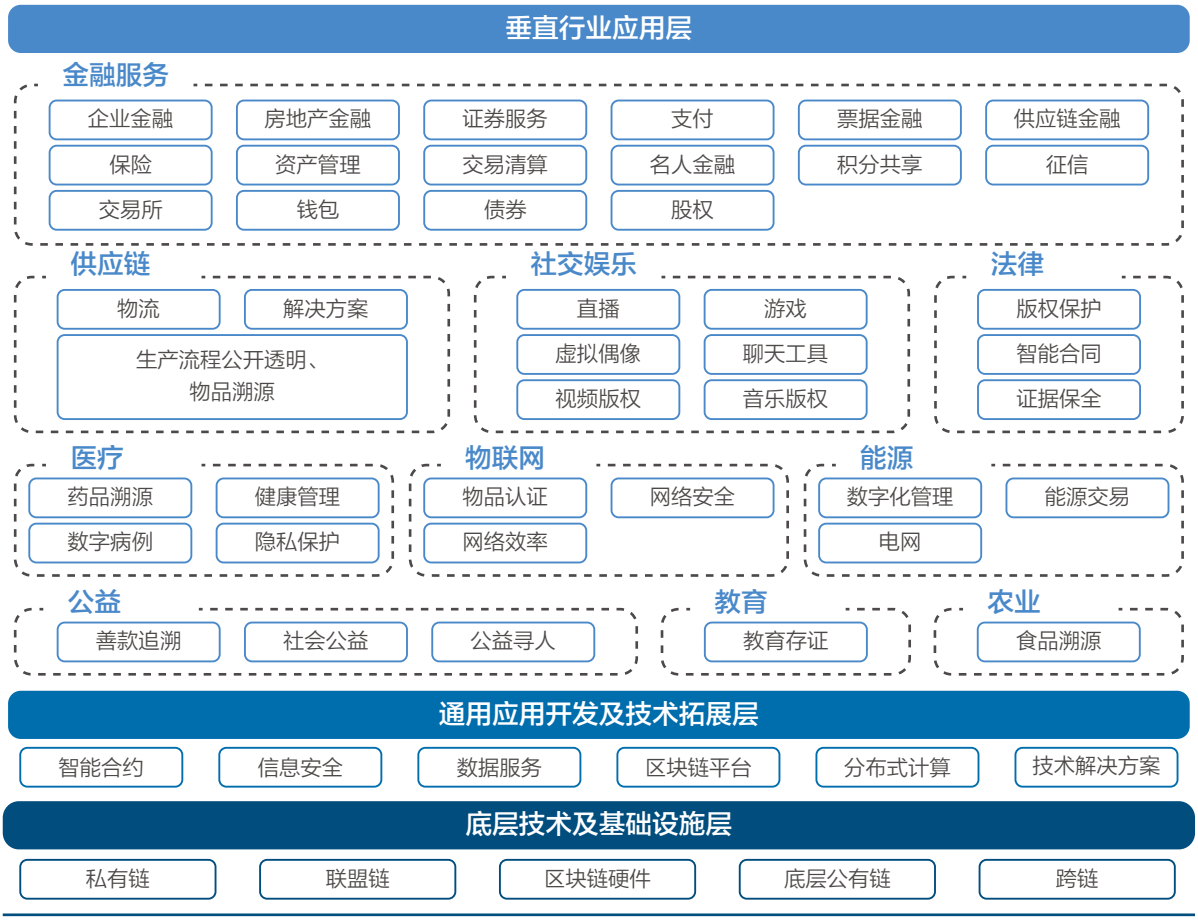
区块链数据由多个不同交易主体相互背书，可以省去人力审核步骤，减少中间环节，节省交易时间，从而提升商业效率。同时，基于区块链的防篡改和可追溯的特性，降低交易风险，减少商业纠纷。

打造新的商业模式

区块链技术将开创非中心化的交易方式，实现可信交易和价值传递。未来，区块链将会产生新的商业模式，不仅降低成本，还能增值赋能。例如，分布式身份识别系统（De-centralized ID,DID），就是新的商业模式之一。借助 DID 技术，可以实现顾客身份的隐私保护，并且提供合理特征帮助企业更好地了解顾客需求，从而为顾客提供定制服务。

区块链的商业图谱

区块链技术的应用已从单一的数字货币应用，扩展到社会的各领域。各应用场景如下面商业图谱所示。



图：区块链商业图谱

区块链有着去中心化、可追溯、不可篡改、数据安全透明等特性，可以解决现有业务的痛点，实现业务模式的创新。

可追溯性

区块链技术的可追溯性适用于各个领域交易信息的管理与监督，不仅确保信息的连贯真实，而且支持监管的及时有效。

供应链领域：商品防伪追溯

正如前文所述，商品防伪追溯是区块链的典型应用场景。而供应链领域是信息不透明、长流程、多环节的典型代表。构建供应链领域的商品防伪追溯可以打造良好的信任生态体系。

区块链技术通过提供完整流畅的信息流、不可篡改的签名认证机制，可以实现去中心化或多中心化的精准追溯和充分信任，天然地适用于供应链管理。通过区块链技术的介入，将商品从原材料生产的过程、流通过程、运输过程、监管过程中每一步的数据都标上自己特有的标识信息，且都附有各主体的数字签名和时间戳。所有数据都被整合并写入区块链，供消费者查询和校验，实现精细到一物一码的全流程正品追溯，同时也实现生产制造商、渠道商、零售商、消费者、监管部门、第三方检测机构之间的信任共享，全面提升品牌、效率、体验、监管和供应链整体收益。

政务及公共服务领域：公益追溯

政务及公共服务的公益监管是基于政策规章、采取抽查方式行使监督管理职责，难以实现全面、及时监控。通过使用区块链技术，搭建包含政府监管机构、第三方公共服务机构的信息平台，从而实现公益信息实时监管，保障每一笔捐助都有源可溯，捐赠人可以通过客户端实时的查询自己所捐赠物资的状态，直接地看到物资整条物流信息的变化以及发放到受助人手中的过程。将捐助者全部的过程信息均使用区块链技术来防止篡改，确保公益透明性、可追溯，将极大增加公益平台的权威性和可信度。

去中心化

区块链技术具有的去中心化特性，可以用来简化操作流程、缩短交易时间，从而降低交易成本。同时，因为区块链技术能够实现点对点的价值转移，所以实现了基础设施架构重建，支持非中心化场景。

金融领域：支付

当前支付完全依赖于金融机构尤其是银行作为中心节点进行交易确认，随后交易行为才可完成，这中间存在大量的冗余流程和时间成本。利用区块链技术的去中心化特性应用于金融的支付领域，有助于降低金融机构间的对账成本，从而显著提高支付速度及效率，这一点在跨境支付领域的作用尤其明显。

新能源领域：数字化管理

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。例如太阳能这类新能源具有多点分布式布局的特点，各个发电企业及用户都可以使用太阳能板来进行发电，各用电单位也可以据此使用电力，通过区块链技术和智能电表相结合，对不同主体的发电量、消耗量进行计算和记录；真正将区块链技术的点对点交易特性充分应用，为社会创造价值。

信息安全透明、不可篡改

当前，各种信息造假、侵犯产权的事情时有发生，进而引发各种经济甚至法律纠纷。区块链技术可以保障相关产权，并从法律层面确认合同及证据的真实有效。

法律领域：合同及证据管理

基于区块链技术，合同签署各方在签订电子合同时，合同以及相关的材料会生成对应数据并在区块链上存证，如发生合同 / 证据造假等情况时，监管部门可快速通过核对链上存证信息，判定造假主体，实现实时监管。

最高法院于今年 9 月 6 日出台的《最高人民法院关于互联网法院审理案件若干问题的规定》[35] 中，已经明确指出“当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认。”。这是国家最高司法机关对区块链技术的认可。

文化娱乐领域：产权保护

区块链技术通过时间戳、哈希算法对作品进行确权，以此来证明作品的存在性、真实性和唯一性。一旦在区块链上被确权，有关作品所有后续的操作和交易信息都会被实时记录，作品可追溯、可追踪，为司法取证提供了强大的技术保障和事实性证据。并且利用区块链技术，可以实现作品全生命周期追溯，从创意诞生到作品最终生成都将被记录在链，从而实现各个环节的有效整合、加速流通。

教育领域：教育存证

区块链技术可以查询跨地域、跨院校的学生信息，用来追踪学生在校期间的所有表现行为，能帮助有良好记录的学生获得更多的激励措施，并构建起一个良性的信用生态。同时，将学生的各种证书信息上链，未来可供第三方验证证书内容是否被篡改，从而确保教育证书的真实性。

上述提到的垂直行业的应用层都是依托于区块链技术和行业结合的扩展。而区块链本身的技术发展，也会产生大量商业机会。如图中所示，可以分为通用应用开发及技术拓展层、底层技术及基础设施层。其中通用应用开发及技术拓展层则包含以智能合约，信息安全，区块链平台，分布式计算和数据服务为重点的多项技术领域，适合技术驱动型企业投入和耕耘。底层技术及基础设施层包含各种链的形式，如基于区块链硬件的私有链、联盟链、公有链以及跨链等，相较上层，底层技术及基础设施层不仅需要大量技术先锋企业，也需要负责未来网络升级维护的传统型 IT 企业，以构建完整的生态；只有基于技术层面的完备，垂直行业的应用层才得以充分开发和利用。

区块链的商业模式

区块链相关的商业模式，比较经典的划分方式就是所谓的币圈和链圈，最近也在两者之间出现了通证派（token），主要淡化数字货币的色彩，而强调通证作为有背书、可流通、加密的数字权益证明在实体经济中的流转作用。在企业级应用中，区块链的商业模式也可以根据 2.2 的内容，分为与行业相关的和与底层架构、平台建设相关的。在具体的应用方式上，有技术先导公司强调技术突破，也有专注平台建设，以联盟方式运作欢迎行业客户加盟的。以供应链为例，有专门从事类公链（基于 ethernum 等源代码修改成的公链）研发，鼓励供应链上下游厂商一起参与的，有以企业联盟为基础联合上下游厂商一起组建联盟链的，也有核心企业牵头并以自己业务为主导构建联盟链的；在具体业务上，有支持采购、生产、物流等综合业务的，也有只强调物流和溯源的单一业务，甚至还有结合金融（保理、贷款、融资、税务）等复合业务的。企业在具体选择商业模式上，应该以自身业务为出发点，综合业界现状，选择合适的模式。

3 联想区块链技术

区块链应用领域非常宽广，联想的区块链技术主要面向企业客户，一直致力于与业务合作伙伴打造共赢的商业网络，给用户、客户提供增值的产品和服务。联想区块链目标就是打造面向企业级的商业网络，针对复杂多变的商业环境，联想给业务合作伙伴和客户提供安全可靠的区块链平台和解决方案。联想从底层开始设计了灵活的架构，可支持不同类型的应用场景，且模块支持可插拔，是一个高度模块化松耦合的区块链系统，支持企业用户选择不同的区块链方案实现。

区块链的架构

联想提供的区块链解决方案，属于典型的联盟链 / 私有链场景。联想区块链架构如图。

图：联想区块链的架构

联想区块链体系架构可以分成三层，即由底层的基础架构层，平台层和上层的应用框架构成。这三层架构划分与云计算的层级比较类似，分别对应了云计算的 IaaS（Infrastructure as a Service, 基础架构即服务）、PaaS（Platform as a Service, 平台即服务）和 SaaS（Software as a Service, 软件即服务）。

底层的基础平台，其支持的物理网络环境多样化。正如 1.3 中提到，一个支持异构物理主机、跨地域的基础架构更符合区块链技术的本质，因此联想的基础架构层与普通的云区块链方案不同。联想实现了对各种存量异构物理主机的支持。

联想针对不同类型的服务器提供统一的虚拟化管理实现，支持从 x86 到 ARM64 的主机。同时，联想还扩展了目前主流的云区块链 BaaS 的实现，不仅支持公有云，还支持企业私有云，以及两者混合的混合云方案。针对主机间互联需要跨越不同类型的企业网络，联想提出了可统一管理，支持跨隔离区（demilitarized zone，DMZ）的 IT 解决方案。基于各项底层技术，最终为客户构建一个物理分散而网络层统一的动态基础架构层，据此搭建的区块链系统将更为灵活和可靠。

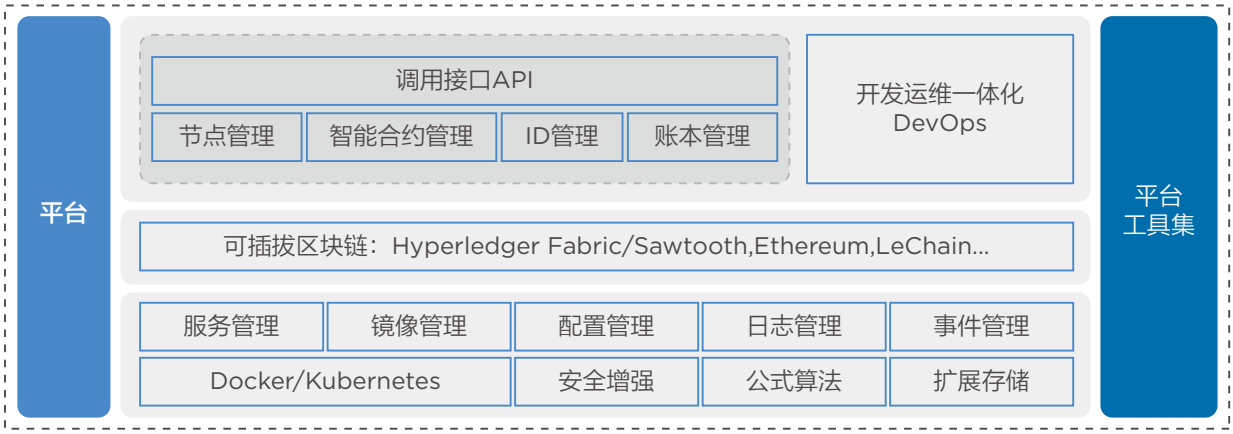
平台层是区块链系统的核心，为系统提供了区块链服务。仿照云计算，平台层的实现常被称为 BaaS（Blockchain as a service）。平台层的架构，由下层到上层依次为容器管理框架、可插拔区块链子系统以及对上层应用的接口 /SDK 部分和开发运维一体化（DevOps）。其中容器管理框架是平台层的支撑子系统，主要基于容器 Docker/Kubernetes 等技术实现对不同区块链的支持和性能的优化。在可插拔区块链子系统上，联想区块链方案可以支持不同的区块链原生方案以及联想的自有增强方案。而基于不同的区块链系统，联想最终为上层应用也提供并扩展了不同的 API 和 SDK，并且提供了开发运维一体化 DevOps 加速集作为开发的快速部署使用。同时，为了更好支持系统维护和相关上层开发，联想也提供多个不同层次的区块链工具集。

在应用层，提供的应用框架主要是针对具体业务提出的整体解决方案，例如提供与行业相关的深度定制方案等。目前联想的区块链已经在供应链等场景中开始商用，针对这些领域可提供参考设计以加速客户的开发和系统升级。

区块链即服务（BaaS）

区块链即服务（Blockchain as a service），其本意是借鉴云计算的概念，希望区块链系统以整体方式屏蔽内部实现的细节、对外提供统一服务，从而降低客户在使用时的管理维护成本。

联想的 BaaS 实现，实质对应是联想的区块链平台，即前一节架构部分涉及的平台层，包括“容器管理框架”、“可插拔区块链子系统”和“接口 API 及开发运维一体化 DevOps”，细化内容如下图所示：



图：联想区块链的平台层示意

其中，容器管理框架，其内容包括基于 Docker/Kubernetes 的管理平台，以及区块链性能扩展系统，包括安全增强模块、共识算法和扩展存储系统。对上层系统而言，容器管理框架提供了包括服务管理、镜像管理、配置管理（用户管理）、日志管理和事件管理功能在内的各项功能。中间层的可插拔区块链子系统，联想区块链平台实现了包括超级账本 Fabric，超级账本 Sawtooth，以太坊以及联想针对 Fabric 的隐私增强方案 LeChain 等在内的多个原生和增强区块链实现。在上层的“应用接口及 DevOps”，提供了包括节点管理、合约管理、身份 ID 管理和账本信息管理在内的多个模块。

主要技术特征

联想的区块链平台，作为企业间高效数据协作平台，为企业客户提供了数据驱动业务的新型 IT 模式，并将助力企业实现行业智能转型。联想区块链平台具备安全、高效和易用三大特征。

安全

高效

易用

在安全上，考虑到商业数据的敏感性，联想的区块链平台重点实现了隐私保护，包括对用户身份、交易数据、智能合约以及合约状态的保护。在保护的同时，方案也实现了对安全审计的支持，对国密算法的支持等，提供了包括密码矩阵在内的一系列安全增强实现。

在效率上，实现了企业间或企业内的多方强协同模式，这比之前传统 IT 的点对点的信息弱协作模式性能提升了很多，而且在业务模式调整、业务流程变化时，极大降低了对已有系统的改造成本，这也就是真正的数据驱动业务新模式。同时，针对各种已有的智能合约体系，安全可信的智能合约将驱动和加速了跨实体的业务数据自动流转。

在易用上，联想区块链平台提供了全流程的可视化工具，使得操作简单，部署快捷。区块链系统作为一种复杂的 IT 系统，其安装难度较大，需要在各节点上安装系统和大量软件，并最终调试、配置等。为了降低大家使用的瓶颈，联想实现了可视化的安装工具，创造性提出了类应用商店的下载模式，能快速远程实现系统的部署。而且本方案底层支持异构的物理主机和各种混合云方案，真正符合区块链的多机、异构精神，同时也支持企业内部渐进改造和升级，最大程度降低了企业 IT 的成本。

基于容器管理框架

现有区块链平台一般都会提供详细的框架搭建、开发文档和工具来方便的让开发者进行研究、探索和开发。但是，在企业级分布式环境下快速的部署、初始化使其快速上线并不简单，例如有着区块链平台、相关工具的配置和调用、区块链网络拓扑的设计、证书和密钥的安全分发、组件和服务的高可用性、业务处理能力的弹性扩展、数据的持久化等方面的考虑和设计，需要开发者和IT团队对区块链相关技术有深入的了解，需要专业和完善的企业基础架构和资源服务的支撑。不仅如此，区块链的配置和部署过程涉及到大量的参数，过程繁琐且互相关联，出错概率很高，需要频繁地进行端到端测试才能确保区块链的正确配置和部署，耗费的时间数以天计甚至周计。在这种情况下，企业无法聚焦于区块链上层应用的开发和业务创新的思考上，极大影响了应用和解决方案的快速迭代、快速上线。这些都是在初期研究探索区块链技术时遇到的实际问题，针对这些问题联想构建了容器管理框架解决方案。

联想容器管理框架是联想公司提供的高性能容器计算平台。联想容器管理框架基于 Docker/Kubernetes 技术搭建，针对行业中容器化应用的需求、结合联想在云平台运营过程中的长期积累，为应用提供了完善的执行环境管理能力。联想容器管理框架支持微服务架构、CI/CD 以及全方位运维监控等高级应用管理功能，配合异构支持以及超融合架构管理，为容器应用的快速落地提供了完整的解决方案。

联想容器管理框架是联想公司提供的高性能容器计算平台。联想容器管理框架基于 Docker/Kubernetes 技术搭建，针对行业中容器化应用的需求、结合联想在云平台运营过程中的长期积累，为应用提供了完善的执行环境管理能力。联想容器管理框架支持微服务架构、CI/CD 以及全方位运维监控等高级应用管理功能，配合异构支持以及超融合架构管理，为容器应用的快速落地提供了完整的解决方案。

联想容器管理框架针对联想区块链平台提供了深度定制化的功能特性，并增强了容器本身的安全机制，为上层区块链商务应用的开发、测试及高效执行创建了完整、可靠的计算环境。

01 区块链生命周期管理

联想容器管理框架借鉴了终端设备应用商店的概念，为客户提供极易操作的应用统一管理方案。通过联想提供的商业应用商店，用户不仅可以实现一键应用部署，还可以完成多应用的统一调度编排、应用升级维护等高级管理功能。

联想容器管理框架为区块链应用提供全生命周期管理服务，包括应用的部署、升级、扩容、多平台运行、服务流量管理等运行时功能需求以及开发、测试、运维等完整的应用开发管理特性。联想容器管理框架将联想区块链平台的底层资源完全透明化，安装、运维都极为简单，使得最终用户只需关注区块链平台之上的业务管理。

联想容器管理框架支持 7*24 全方位监控服务及实时告警功能。联想容器管理框架将持续监控联想区块链平台的资源使用情况、服务健康状态，并根据用户配置及时扩容平台，保障应用的高效执行。当检测到应用错误时，联想容器管理框架将实时报警，并进入预先设定的自动错误恢复流程。

02 平台高可用

联想容器管理框架为上层系统中的关键组件设计了多副本执行机制，并支持每个组件副本执行在不同的服务器上，使得单个组件副本的错误不会影响到计算框架的可用性，从而提升了区块链底层服务的鲁棒性和安全性。同时，联想容器管理框架也实时监控联想区块链平台各底层组件的执行状况，为将出现的错误状态提供预警功能。针对联想区块链平台的问题组件，联想容器管理框架将及时创建新的组件进行替换，保证应用各个组件的高可用。

联想容器管理框架的高可用存储方案基于软件定义存储模式设计。基于此，联想容器管理框架将所有机器中磁盘设备聚集成存储资源池，并通过多副本、全局负载均衡、错误恢复等多种针对性技术手段为容器管理框架中应用的存储需求定制专用的高可用存储解决方案。除此之外，联想容器管理框架将容器编排平台的存储设备接口与存储资源池的存储供应接口提供了协同优化，从而为联想区块链平台的执行、迁移、扩展等操作提供了高效可靠的存储需求支持，保证用户业务的高效稳定运行。

联想容器管理框架的高可用网络系统为底层计算资源及网络资源池提供高效、稳定的网络解决方案。联想容器管理框架网络系统从硬件冗余及软件设计两个方面满足网络系统的高可用需求：网络系统从网络硬件上进行冗余设计，无论是节点网卡、物理交换机等，在网络通路上的所有物理设备都将进行冗余配置；软件方面，联想容器管理框架网络系统提供了强大的网络异常检测及网络错误恢复功能，极大地增强了计算框架中网络的可用性。

03 异构支持

联想容器管理框架支持异构服务器以及硬件加速器组成的异构集群和混合云。区块链平台上的应用组件可以执行在不同架构的服务器上，充分利用异构服务器、混合云提供的计算特性以及硬件加速器带来的性能提升。

异构服务器主要是支持了 X86 和 ARM64 两种 CPU 类型的服务器。这是两种目前主流的企业级服务器。一般企业多使用 X86 的 CPU，也有行业则使用 ARM64 的服务器。联想的容器管理框架可以同时运行在这两种异构服务器上，做到了互联互通，协同一体。

混合云融合了公有云和私有云，是近年来企业级云计算的主要模式和发展方向。私有云主要是面向企业用户，这是因为基于安全考虑，企业更愿意将数据存放在私有云中，但是同时又希望可以获得公有云的计算资源，在这种情况下混合云被越来越多的采用，它将公有云和私有云进行混合和匹配，以获得最佳的效果，这种个性化的解决方案，达到了既省钱又安全的目的。利用和各云服务商新建的大量的网络资源，业务根据业务场景和用户选择不同的云平台。联想容器管理框架支持在不同云平台和私有云之间将区块链项目部署上线，不管公有云平台还是私有云平台，区块链节点之间的调用都支持内网中高速互联，这样降低了网络延时，提高了业务交互效率，提升业务价值。

异构集群对区块链平台的运行是透明的。联想容器管理框架将根据当前应用的需求将平台组件部署到相应架构的服务器和混合云上，从而提升平台的可靠性。除此之外，联想容器管理框架还优化了平台的调度策略，从而提升了整个计算框架的性能表现。

安全增强机制及隐私保护

区块链作为一种新兴数据共享技术，其数据机密性和隐私保护问题是应用场景中急需解决的重要问题。联想区块链安全隐私从以下方面提供更强保障：

01

两级安全证书机制

区块链可以提供防篡改，去中心的服务，参与交易节点的身份隐私十分重要。公链中的用户可以使用公钥哈希值作为唯一标识，但是攻击者仍然可以通过对具有关联性的区块链地址进行聚类分析，获得有价值的信息。联盟链身份管理服务多采用 PKI 体系，但是证书会将用户的真实信息完全暴露在区块链系统中。因此无论是公钥地址的隐私保护机制，还是联盟链基于 PKI 的证书体系，均存在交易可关联，身份暴露的问题。联想区块链提供一种既可以满足交易匿名又可以实现后台身份监管的两级证书机制。联想区块链的两级证书机制保护了用户的身份信息，并且在满足交易身份对未参与方保密的同时，监管者可以监管全部交易方的身份信息。

02

针对指定交易内容的加密

区块链上的每个节点都保存了一份完整的区块链账本副本，账本上的数据可以被任意检索和查询，而且数据本身是没有加密的，所以区块链对于网络节点是公开透明的。虽然区块链的公开透明性为各节点对数据的验证带来了方便，但同时也带来了严重的数据隐私泄露问题。联想区块链提供了一种针对交易记录中任意内容加密的安全机制，对数据可实现任意粒度的隐私保护。区块链中的节点账本上保存的数据都是加密之后的数据。使得敏感数据只对有权限的用户可见，非权限用户查询得到的数据只能是密文。即使保存敏感数据的节点是恶意节点或者节点被攻击，也无法得知敏感数据的明文信息。

03

同态加密算法

与传统加密技术不同之处在于同态加密不需要数据解密就能对数据进行操作。同态加密与明文进行同样的运算再将结果加密一样，允许对密文进行特定的代数运算得到仍是加密的结果。联想区块链提供同态加密库，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，最终账本保存的是加密之后的密文数据。即使节点被攻破，获取到账本记录也无法解密。

04 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。联想区块链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。

05 可信执行环境

区块链为互联网上的价值转移创造了新的基础。可信计算为设备上的受保护执行创造了基础。可信执行环境（TEE）是可以被验证并被证明在参考条件下运行的安全环境。联想区块链利用 TEE（如 Intel SGX），创建可信的网络。TEE 环境既可以证明放入代码的正确性，又能保证运行时内部数据对外界不可见以及不被篡改，进而可以确保保障区块链协议关键代码和数据的机密性、完整性，使得区块链的应用可以在完全受信任的成员节点上高效运行。

共识机制与性能

在区块链系统的理论中，共识机制是核心。所谓共识，就是通过某种算法（规则）去保证多节点的数据、状态、行为达到一致。共识并不考虑数据业务逻辑的正确性，只需要考虑每一个结果是不是能代表“大多数”参与者（网络中的各个节点）的意见，从而最终达到一致。

在分布式系统的理论与实践中已经存在不少优秀的算法，如：Paxos，Raft，PBFT（Practical Byzantine Fault Tolerance，实用拜占庭容错）等，这些算法多用于分布式存储或者日志系统。而比特币作为公链的代表，使用的是 Proof-of-Work（PoW）的概率共识机制去达成分布式账本的最终一致性。

目前来说，主流共识的算法可以根据场景分成两大类：

01 可信节点的共识机制

在一个分布式系统中，如果所有节点都是可信的，说明该系统中只存在网络延迟或者节点瘫痪的现象，不存在恶意 / 作弊节点。此时，只用满足 Crash Fault-tolerant（CFT）的容错需求，如 Paxos，Raft 等，虽然容错能力不是很强，但是运行效率高。这种共识机制多适用于联盟链和私有链，并不适合网络环境复杂的公有链。

02 不可信节点的共识机制

这一类共识机制，可以容忍恶意 / 作弊节点，支持拜占庭容错 Byzantine Fault Tolerance（BFT）。此类共识机制既可用于开放的公有链，比如 Proof-of-Work（PoW）、Proof-of-Stack（PoS）等，也可用于联盟链，比如 PBFT 和 SBFT（Simple Byzantine Fault Tolerance，简单拜占庭容错）等。

联想在共识机制上主要有如下两大技术特征：

01 算法创新

共识机制和共识效率，是区块链系统的灵魂。从最初的 Paxos 和 Raft，逐步发展到今天的 PBFT 等算法，虽然已经有许许多多的共识算法尝试满足不同业务场景的需求。但还是存在很多不可忽视的问题需要去解决，比如节点数量的可拓展性不足，交易吞吐量不高，容错程度不高等问题。许多新兴算法都在尝试去更好地权衡性能和去中心化的关系。

实用拜占庭算法 PBFT 首次提出在异步网络环境下使用状态机副本复制协议，而且通过多种优化，解决的 BFT 难以工程化的问题。而且通信复杂度下降到了 O(n2)，PBFT 能在 3f+1 个节点集群内容纳 f 个发送恶意错误信息的节点。

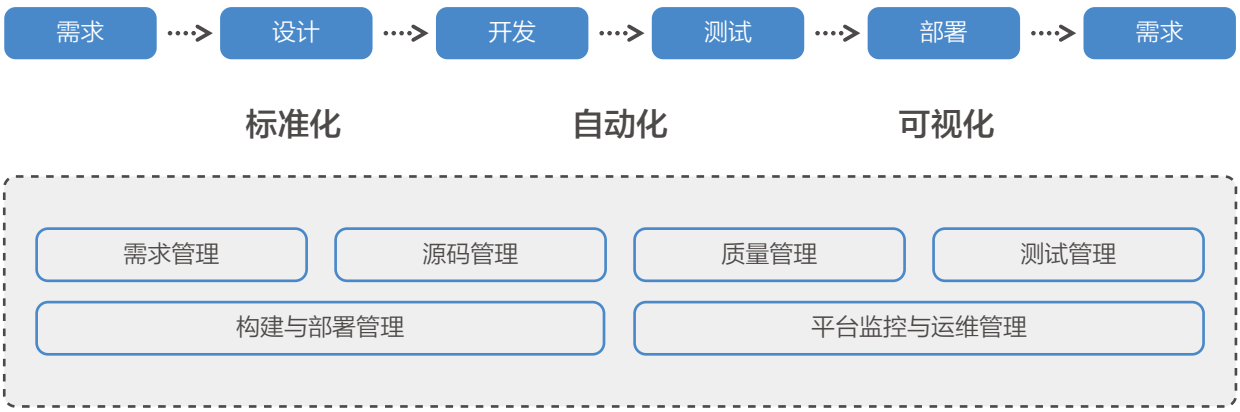
同样的，PBFT 也存在不少问题，比如繁重的签名校验和冗余的通信，频繁的 ChangeView 更新主节点，都会严重影响共识的性能。联想区块链为了解决这个问题，引入了不同类型的加密和消息验证方案，利用自主研发的简单拜占庭 SBFT 算法去让 PBFT 的工程化更加容易实现，而且同时能保持一定的鲁棒性和交易处理性能，降低通信复杂度。

02 架构灵活

联想区块链基于模块化实现了系统层级上的可插拔共识机制，通过开放的数据接口，可以支持各种主流的共识算法。包括 Raft、PBFT，SBFT 以及 PoW、PoS 等公链主流算法，都可以接入到当前系统中，可以真正的做到共识的可插拔化，甚至是未来的跨链通信。这个结构的创新给予了联想区块链在未来的无限可能性。

开发运维一体化（DevOps）

基于对不同应用的实践经验，构建持续集成，自动测试和持续部署平台，实现标准化，自动化和可视化的 IT 实施管理框架。联想区块链平台支持从开发、部署到运维测试全套自动化流程。应用开发人员对代码的修改可以触发项目的源码编译、应用打包、并且部署到联想区块链平台中。同时，区块链平台将启动一系列单元测试及集成测试，验证应用的正确性，并将测试报告反馈给开发人员。



图：开发运维一体化示意

区块链平台支持灰度升级及蓝绿部署，并且支持多版本应用实例。在应用升级的过程中，区块链平台可以将应用流量逐步迁移到新版本应用中，以实现应用的平稳升级，保证应用升级过程中服务可用。当应用升级失败，平台可以将应用回滚到旧版本状态。

区块链平台提供了完整的日志聚合及分析功能，基于 AI、大数据处理技术，平台能够深入分析区块链应用可能出现的错误模式，并及时向用户发送预警信息，保障应用的稳定高效运行。

区块链的应用框架

在当今企业的商业网络中，各合作伙伴拥有自己的企业系统架构和应用。无论是独立部署还是云部署，各企业的企业架构都是独立于其他合作伙伴，即便他们之间有协同或集成。相对于整个商业网络而言，这些架构和应用都是企业私有的、定制的，从而导致企业在协同时需要投入大量的工作和资源，严重影响了企业间效率的提升和合作关系的深化。

区块链是由共识协议保证的、不可篡改的、促进多方信任交互的、共享的分类账执行系统。区块链应用的目的之一就是从基础上去解决企业商业网络间的协同效率低下、成本高昂和无法建立彼此信任问题。区块链记录的不可篡改特征从根本上降低交易风险，并最终促进建立安全可信的交易、建全公平交易环境，从而服务各种企业场景尤其是依赖信任的商用场景。

联想区块链应用框架是联想对区块链技术的不断探索和实践中逐渐形成的，是基于全球业务部署，在考量全球各地业务风险控制、业务合规和业务流程管控等基础上搭建应用于全球业务的区块链网络平台。

通用应用架构

区块链网络是一个可扩展、可伸缩的网络，各节点、组织可以根据实际业务需要加入和退出相应的区块链联盟。区块链应用架构设计需要考虑：

01

柔性的成员类型和成员进出机制

企业级区块链有多种形成方式，或由某个核心企业发起，或由行业联盟发起，或由某个云服务商发起等。总之，网络形成多种多样，规模由小变大，由业务驱动，由于企业业务的变化和企业间业务的增减，都会导致网络成员的增加和减少。在业务的生命周期里，业务的参与方不仅包括实际资产的直接交换方，还包括银行、物流、监管、审计等，业务参与方是多样的。这些就决定了在区块链网络设计之初需要考量成员的多样性和网络的成长及伸缩能力。

01

公平和共赢的网络

区块链应用是架构在企业 / 组织间的透明的、共享的和可信的交易数据基础之上，可以帮忙参与各方降低运营风险，提供给可靠、实时和可预测的数据，降低合规成本。由于区块链数据是透明且共享的，因此整个应用要求参与各方建立一个公平的合作环境。在应用区块链时，参与各方的商业利益实现及价值增值是维护网络发展和健壮的重要因素，参与方在网络中的运营成本也是网络维护的关键因素，只有区块链应用不断给参与各方带来成本节省和利润增加，整个应用平台才能健康发展。因此，区块链应用必须确保提供各参与方一个公平和共赢的合作环境。

01

网络治理

区块链应用维护是维护网络运转和健康发展必不可少的组成部分，区块链应用维护不仅只包括技术架构治理，还包括数据标准、数据安全级别、智能合约和业务流程等。在区块链技术发展初级阶段，同一个区块链网络要求各节点具有统一的技术架构和软件组件版本，这样才能保证共识的过程和账本的一致。企业级区块链网络中的数据是共享的，各参与方需要具有统一的数据标准；数据按安全准入和权限级别控制的，因此数据的数字签名规则、数据加解密算法需要全网统一。智能合约部署需要各相关方对合约规则具有统一的协议，共同批准代码的实现、变更和终结并进行数字签名，避免智能合约的争议。网络中数据是共享的，业务流程也从过去企业内独立转变为企业间协作统一，同时也要求企业内和企业间业务流程具有相同的数据颗粒度。

01

共识协议

信任是区块链技术的本质，是区块链应用各参与方投入建设平台的基础。信任需要通过各参与方共同验证交易的可信性并达成共识。共识是一个过程，共识需要机制及其算法来保证。在设计一个区块链应用及账本时，就需要考虑对应的共识协议，需要各方都信任的共识机制，这样才能不引起各方争议，才能逐步形成区块链网络生态。

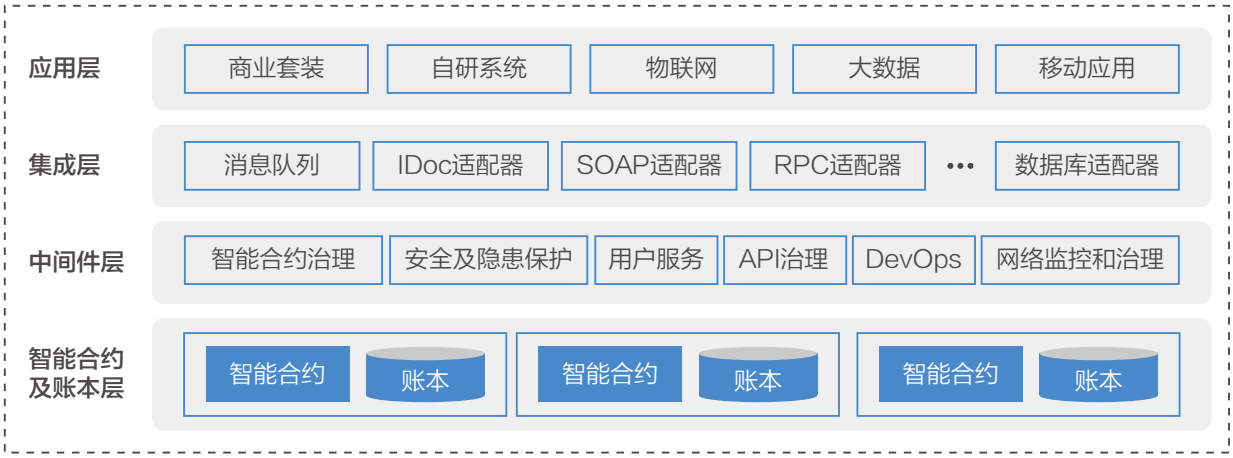
01

安全服务

区块链技术中的安全来源于人类对于数学的信任，基于数学理论的加解密方法确保区块链数据的所有权可信并不可篡改。在企业级区块链网络中，由于参与方的多样性和交易行为的复杂度，要求区块链网络做到安全、透明和权限控制。为了保证交易和资产的安全，区块链网络需要支持不同安全级别来保证区块链的信任水平，比如 CA 证书机制及用户 PKI 体系、数据安全加解密、智能合约加密、安全合规（例如，欧盟的通用数据保护条例 GDPR,General Data Protection Regulation[36]）、网络安全等。

以上几点都是区块链应用框架设计需要重点考虑的方面。在区块链技术发展初期，区块链应用都是带有行业特色、联盟特色的合作网络，因此，在设计时，不仅需要考虑网络间各组织、节点通用和共有的功能和特性，各组织、节点还需要考虑其自有功能和特性。

联想区块链应用架构是基于联想全球业务架构，面向不同种业务网络场景设计，充分发挥区块链价值，实现联想商业网络共赢。联想区块链应用框架采用分层架构设计，具体而言，包括智能合约及账本层、中间件层、集成层、应用层等。



图：应用框架的架构

智能合约层及账本层是按照业务特点进行设计和管理，根据业务流程进行划分，根据不同业务形成独立的账本体系，不同业务可以相互沟通和参考。根据业务进行划分，可以聚焦业务各参与方的交互，避免不必要的数据存储。智能合约是针对具体业务，参与各方共同制定的业务可执行规则和条款，在区块链中，把这些共同制定的合约和条款按照业务流程生成智能合约。因此，智能合约天然就是多方参与和制定，参与各方必须一起制定、审核和签署合约，合约转换的计算机代码也需要参与各方进行审核和电子签名，并同时确定共识过程中背书的规则。

中间件层实现了区块链服务化、服务松耦合、可扩展，区块链按需定制和扩展，智能合约、API 的快速开发和部署而设计。区块链可以根据业务进行账本划分，松耦合的智能合约和 API 可以帮忙业务快速部署新业务和变更。

集成层是沟通企业已有业务交易系统、分析系统、大数据平台、IoT 平台等企业已有系统的桥梁和纽带。集成层提供数据进出区块链网络的各种所需途径 / 适配器，由于企业系统建立于不同时期，其包含多种多样的接口技术，如需跟区块链进行交互，就需要通过对应适配器进行数据格式转换，以满足 REST API 和对应系统对数据格式要求。由于区块链技术是一个基于状态机的异步处理过程，对于从区块链下来的数据，如需进入对应的交易系统或者大数据平台，就需要建立数据消息的缓冲机制，目的使数据不会在系统异常状态下丢失。

应用层包括和区块链网络进行数据通信的企业已有业务交易系统、分析系统、大数据系统、IoT 系统等基于传统 IT 架构的系统，也包括直接建立在区块链上的分散式应用系统和服务（DApp,Decentralized Application）。DApp 是运行在区块链网络和智能合约之上，来获取数据和处理数据的应用程序。企业级 DApp 一般是属于对应企业的单体应用，企业单独开发和部署并可以独立进行。

由于区块链网络是运行于企业间，企业间数据共享就需要一个统一的会话标准，同时，考虑到网络的可扩展性，因此，公共数据治理和统一是非常重要的一个环节。一般公共数据应遵循下面三条原则：采用国际通用标准作为数据语言；采用行业标准作为数据语言；遵循源数据优先原则。

区块链与传统 IT 架构的整合

传统 IT 架构系统指传统企业内部的业务交易系统（ERP、SCM、CRM、SRM、PLM 等）、大数据系统、分析系统、IoT 平台、AI 平台等，包括企业独立部署和云部署。目前，大部分企业都运作在这些传统的 IT 系统之上，它们是企业信息化和数字化的核心，它支撑着企业的整体运营。区块链网络与已有 IT 系统共存设计是非常重要的环节，集成整合要包括业务整合和技术集成，这些整合的成本也是区块链部署中非常重要的一部分，因此，区块链和传统 IT 架构的整合是区块链在企业部署的关键。

在企业 IT 网络中，各企业拥有自己独立的私有系统。各 IT 系统运行着本企业的业务逻辑和数据。企业间通信和信息交换采用 EDI、API 等方式进行协同，个别企业也提供 web service 甚至门户网站实现与自己的直接合作伙伴的信息交换和协同，这些企业间协同方式是企业内流程的延伸，是中心化平台的扩展，并不能真正实现数据在企业所在商业网络的协同和共享。

区块链作为新技术，要想给企业带来真正的价值，并不断创造新的价值，就必须和企业现有 IT 系统进行集成和交互，区块链和企业现有 IT 系统的集成技术和联想区块链技术白皮书（2018 版）联想区块链技术和方案，直接影响到区块链在企业的落地，影响到区块链的价值发挥。因此，在区块链发展的初级阶段，如何和企业现有 IT 系统整合并融入企业 IT 架构，将会影响到区块链在企业应用的成败。

区块链网络可以天然架构在企业的商业网络上，促进商业网络的协同和共赢。区块链可以承载日常企业各自系统的交互数据，也可承载促进彼此信任和更紧密协同的数据。例如，企业 A 和企业 B 存在买卖关系，企业 A 会向企业 B 下采购订单，采购订单发给企业 B 形成销售订单，在区块链上，企业 A 和 B 可以形成一张单据，企业 A 可以用自己现有系统的采购订单进行交互，企业 B 可以用销售订单进行交互。

区块链技术处于技术发展的初级阶段，由于本身整体的分散式的架构及单节点的集中式数据存储，对数据的处理又是采用异步的共识过程，某些性能指标弱于传统集中式架构系统的处理能力，例如，每秒事务处理量 TPS（Transaction Per Second）。因此，需要在链上数据分析和处理时需要考虑这些限制，不应盲目追求各种功能都在链上解决。

在区块链技术发展的初级阶段，区块链能否在企业成功应用，对区块链技术在企业定位很重要。虽然区块链技术前景广阔，但在企业改造时要充分验证、分步切入。现阶段，区块链技术不是传统 IT 系统的直接替代者，它更像是传统 IT 系统的助力者和赋能者。核心企业可以利用区块链技术建立企业的商业网络，促进商业网络各业务合作伙伴的协同和共赢。区块链不仅仅可以链接企业的直接业务合作伙伴，还可以延伸到业务链条的全链，而随着上链企业的逐渐增加、链上生态的逐步完善，其规模效应将会更加显见。

在商业网络中，业务合作伙伴之间按照统一的标准共享交易数据、各级产品数据，消除传统的协同冗余流程，能更好的发现和解决交易中的问题，解决彼此的痛点，降低运营成本，进而加强合作关系和信任，切实的实现协同共赢。商业网络合力一旦形成，将会促进商业网络整体竞争力，改变竞争环境，进而使最终客户受益。

区块链与大数据、AI 关系

区块链网络形成以企业为中心的商业网络，提高了企业间的协同效率，增进了合作伙伴之间的信任，凝聚了企业的商业信用，提升了企业间的合作关系水平。直接带来的好处就是会有更多可信的数据经过区块链传输，更多实时的数据可从区块链获取。这些数据有结构化数据和非结构化数据，这些数据可以直接从区块链引流到大数据平台进行数据分析，大大提高了数据的质量和效能，最大化的发挥区块链和大数据的协同效应。

数据也是智能化变革的最大挑战。联想总结智能化变革有三大要素，数据、计算力、算法。对于企业而言，计算力可以采取购买、租赁甚至升级的方式获得；而算法，可以通过版权转让、外协开发、开源代码等方式。唯有数据，很难快速获取，许多企业都是靠长时间的商业运维中慢慢积累相关的数据，也形成了事实上的数据寡头。数据已经成为企业最核心的资产之一，这也决定了企业间很难共享数据。因为数据一旦共享，非常容易被复制而且很难溯源。企业级阻碍数据共享的另外一个重要因素是数据的价值不明朗，缺乏合适的转让和评价体系。而区块链技术，尤其是充分考虑隐私保护的区块链技术，就能完美解决上述问题。区块链技术保障了数据在不离开属主的前提下，实现数据的共享，并且实现了后继价值的跟踪和追溯。一个典型的实现，就是借助分布式训练模式，将人工智能模型分别在各数据属主那里训练，然后将计算结果分别上链。这样，数据没有离开属主而实现了对全体参与方数据的训练，而且最终的训练结果中，很容易计算各自的贡献度，并且借助区块链还能实现未来收益的再分配。因此，借助区块链技术实现了企业间敏感数据的合理共享，使得企业的数据可以变现，基于数据联合，也将打破了数据寡头对行业的垄断，并共享未来的收益，从这个意义上讲，区块链完美解决了 AI 和大数据的问题。

4 联想区块链应用解决方案

基于区块链的不可篡改、分布式存储的特性，联想围绕自身业务场景，在端到端的业务流程中，使用区块链技术优化业务模式，逐步实现向新型商业网络的变革，并在此基础上有力推动联想智能制造的发展规划。

区块链应用的典型特点

在区块链进入新的发展阶段后，如何寻找业务落地场景正在成为各方探索的重点。联想在推进区块链应用的过程中，也总结出区块链应用的三个典型特征。

增强数据信息透明化

共享账本的数据记录方式将传统点对点的数据集成方式变为分布式的共享记录，避免了集中式存储存在的安全隐患、网络复杂等缺点，增加多方数据透明化程度，为搭建数据集成平台提供了新的技术方案。

降低流程复杂度

区块链在优化多方交易业务流程方面具有广阔的应用场景。传统企业内部为了实现交易完整性往往设置各自流程，在引入区块链技术后，其采用的分布式的数据记录方式，可以共享企业间的业务状态和数据，借助智能合约能快速完成企业间业务流程自动化，为多方交易去掉冗余环节。借助数据共享，还可去除信息不对称引起的多方数据重复核对和审查场景，降低出现交易摩擦的可能性。从一定程度上说，逐步改进业务流程是企业进行区块链改造的关键。

增强交易信息可信度

在区块链共享账本上存储的交易信息数据，在经过哈希加密、按序记录以及分布式存储等方式处理后，具有不可篡改的特性。这些可信的交易信息，可以作为多方交易的审计、金融行业融资等其他更多的使用场景提供数据支持，从而为基于信任基础建立的业务场景提供新的解决方案。

针对企业环境，区块链应用综合考虑上述三大特征，通过逐步实现对传统业务模式的变革，最终发挥出其区别于传统技术的优势。

典型应用场景

从上述特点出发，联想现行的主要应用领域包括供应链管理、销售渠道管理以及供应链金融。

表 4-1 联想区块链典型应用领域

应用领域	典型场景	描述
供应链	交易业务管理	已采购典型流程为起点，利用区块链简化传统业务流程，提高交易数据透明性
销售	渠道销售管理	实现渠道交易数据共享，打通交易各个环节，搭建交易及信用信息共享平台
供应链金融	供应链融资管理	围绕企业的交易联盟链，打造快速、实时、可追溯的供应链融资平台

交易业务管理

背景介绍

联想供应链中存在原材料交易业务管理，涉及联想、代工厂、供应商等多方的物料采购和付款业务。联想为了控制代工厂的成品质量和价格，需要为代工厂指定原材料的供应商，一方面实现产品品控，一方面通过与供应商签订批量采购合同，降低原材料采购价格，最终降低代工厂成品的制造成本。

业务痛点

由于现有业务模式存在多方的采购信息、付款信息和物流信息互相传递的场景，容易造成交易过程中出现产品库存差异、付款周期延长、订单状态未知等问题。各方业务人员需要投入大量的人力完成账目信息的核对，订单状态的跟踪等工作，同时投入大量的 IT 开发和维护成本，才能建立起传统的集成信息系统。造成此类问题的根本原因在于信息不透明，业务流程繁琐：

01

代工厂为联想生产设备，需要通过联想采购原材料，由于无法得知供应商接受订单的时间和供应商的发货状态，将影响其生产计划的制定；

02

联想需要控制代工厂产品流程和质量，需要参与所有物料交易过程，因此联想作为买卖交易的中间环节，带来大量的信息核对和沟通工作；

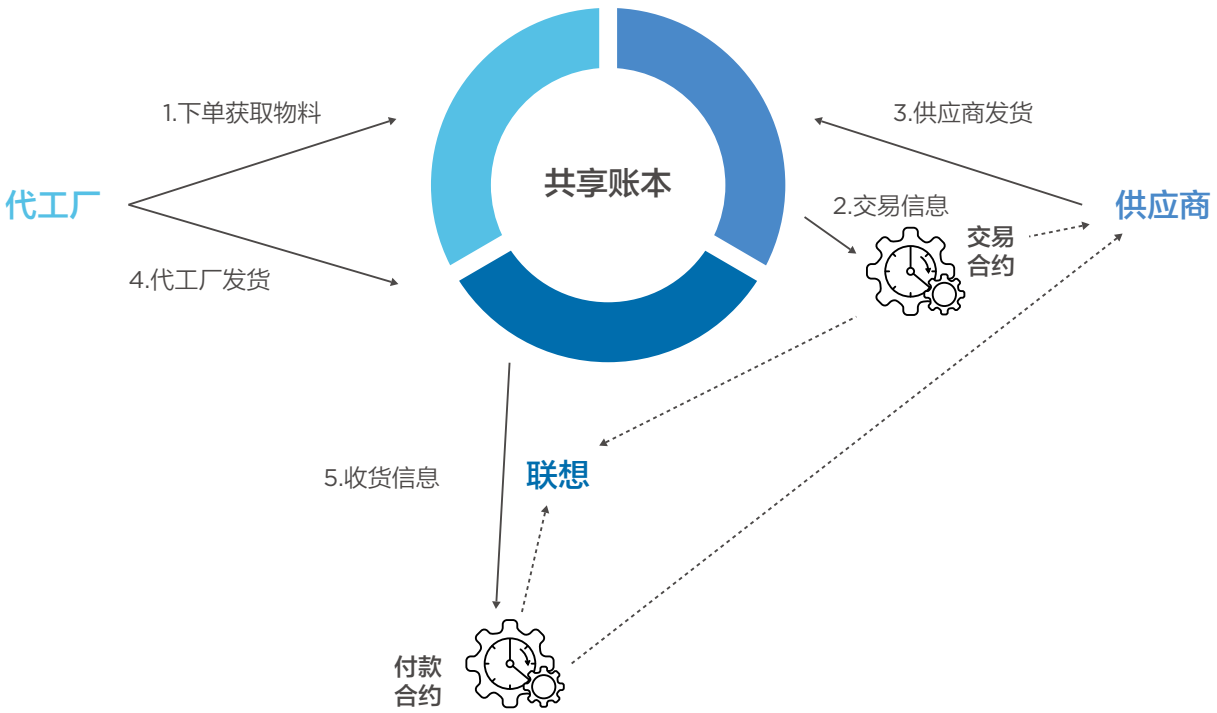
03

供应商作为原材料提供者，在接收到联想的订单后，会将货物直接发送至代工厂，造成联想不能及时掌握具体的收货时间，影响后继流程。

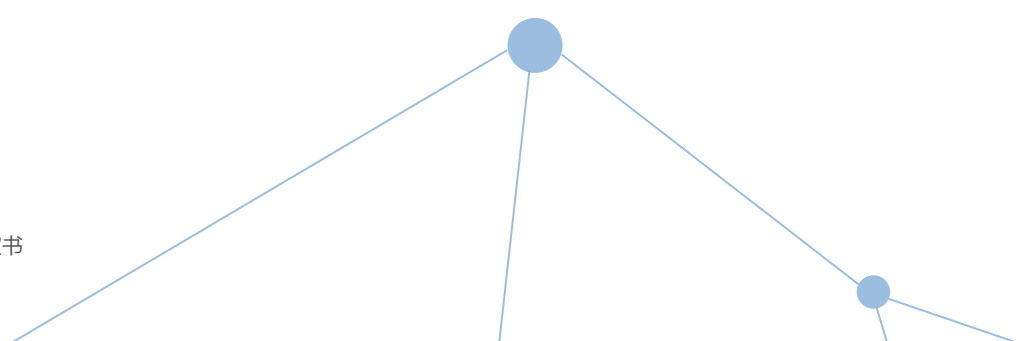
区块链解决方案

区块链技术具备的去中心化特点，提供了快速数据共享的技术手段。针对交易业务流程，联想提出了一种基于区块链技术、简化的、高效的解决方案。具体流程包括：

代工厂直接在区块链上创建的交易请求，分别要求相关方对交易进行核实并背书；智能合约会触发联想业务流程，联想据此选择对应供应商，并记录在链。供应商按照订单完成物料准备后将物流信息同样记录在链。最后，代工厂确认的收货信息将触发区块链的后继合约。该合约根据收货状态，触发联想和供应商的业务系统，并启动最终付款流程。



图：基于区块链的联想买卖业务解决方案



业务变革

针对此类需要通过中间方（例如上述案例中的联想）进行控制的业务流程，联想正在尝试区块链降低信息传递成本，提升工作效率。通过账本共享的方式，将需要中间方确认和核对的信息放在区块链上进行记录，增加多方交互过程中的信息透明化程度，同时利用链上数据触发业务流程的自动化处理。将传统的中介式的流程监督和处理形式，逐步转变为多方协作的、基于物权转移的交易模式，完成对传统业务模式的变革。

不仅在交易管理业务上，联想还在跨国票据的信息共享与传递、电子软件版权采购业务等供应链领域的应用场景中进行了积极探索，在实践中不断扩展区块链商业网络的范围和应用场景。

技术挑战及应对

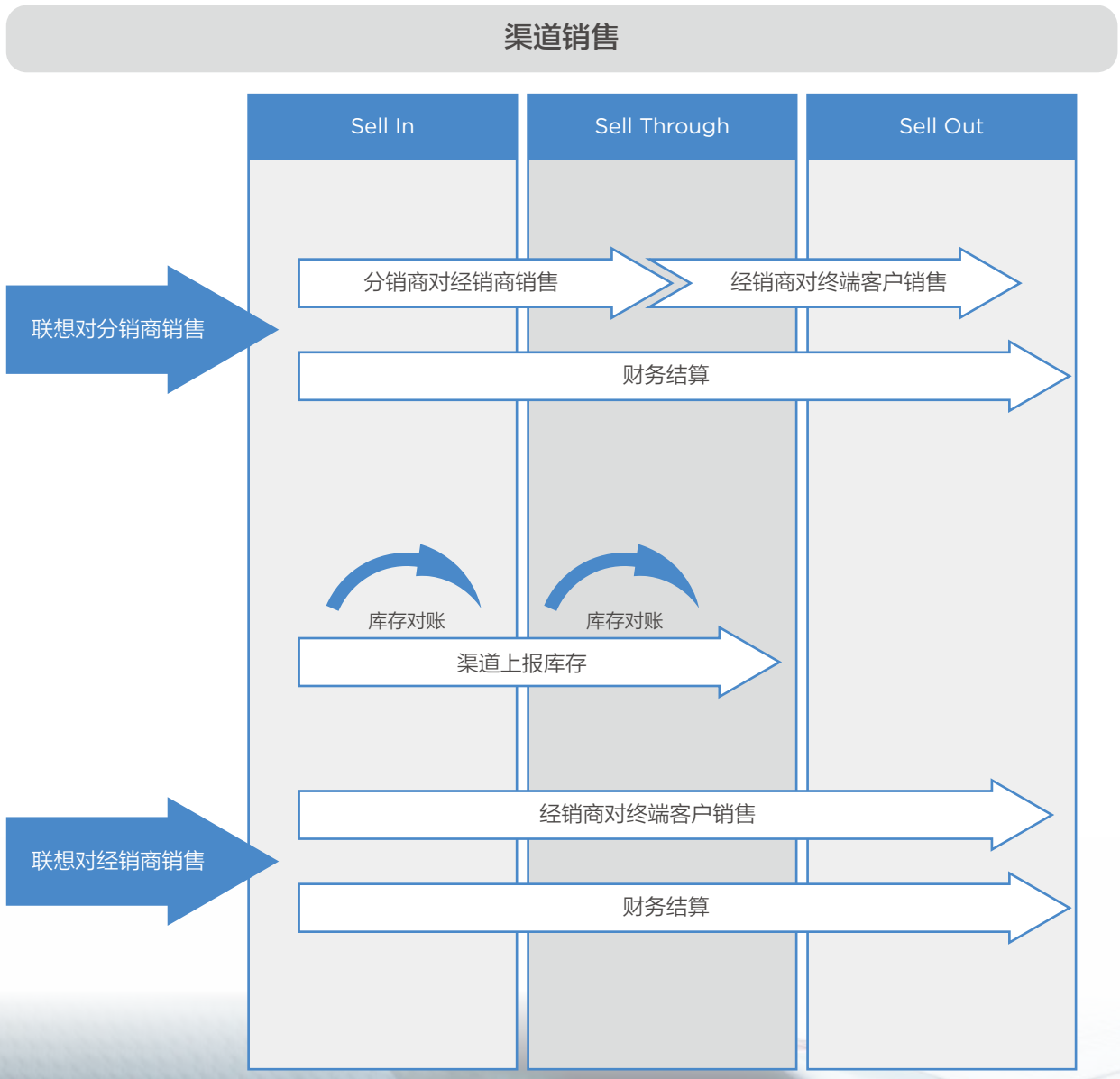
在项目的实施过程中，对于多方交易数据的隐私加密已经成为各参与方关注的焦点问题。现有区块链普遍使用的通道功能，能够将不同参与方的交易数据记录在不同的共享账本，由此对交易数据进行隔离，能解决核心企业需要与单一供应商共享数据的隐私问题。但是对于多方交易数据中只有部分字段需要加密的场景，只能在线下进行加密后再传递至区块链，或者直接不上传此类敏感字段。这将影响到区块链的使用场景，从而对联盟链灵活的加密方式提出了更高的要求。联想提出的解决思路是基于指定字段和指定数据的可选加密方案，解决了上述问题，实现了多方交易过程中任意数据字段的加密问题，从而确保了交易数据的隐私不被非授权用户得知。联想不仅实现了对交易数据的加密访问，还引入了对交易身份的保护，对交易状态的保护等，从而实现了供应链系统中全隐私保护。

渠道销售管理

背景介绍

渠道销售即采用渠道作为销售中介。渠道销售管理主要包括如何开发与选择渠道商，渠道商的日常管理、维护等。渠道作为企业的重要资产，是指生产企业把产品向消费者转移的过程中所经过的路径。这个路径包括企业自己设立的销售机构、渠道商、经销商等。智能制造行业通常有较为庞大的渠道销售体系，因此作为源头的生产制造企业如何更好地管理和维护渠道，打造完善的销售网络，并与渠道商合作共赢，成为了企业运营的关键问题。

联想作为国际化智能制造企业，拥有庞大的渠道销售体系。例如，联想数据中心业务在北美就有 3 万余家渠道商，其中近 50 家为一级分销商，其余为二级经销商。实际渠道销售的业务中，往往是渠道商将联想产品销售并交付给终端客户，联想为了能够快速为终端客户提供高质量服务，通常需要渠道商汇总上报商品渠道流转数据（sell through）和商品终端销售数据（sell out），联想再基于此部分数据制定未来销售计划，进而制定合理的采购、生产计划以缩短产品供货周期。联想渠道销售流程如图示。

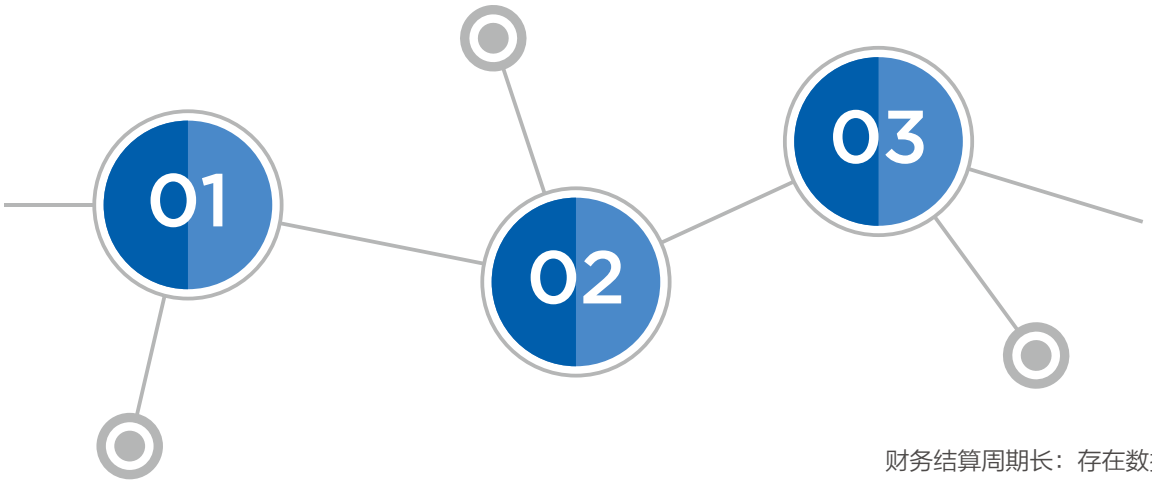


图：联想渠道销售流程示意图

业务痛点

分析可知，支撑此业务需要联想和全体渠道商进行大量的数据交互，传统模式主要是借助系统集成和渠道手工上传数据进行数据收集，但存在如下痛点：

数据的实时性及准确性低：手工上传方式无法保证数据的实时性及准确性，导致联想需要花费大量的人力、时间成本进行数据校对。



企业 IT 开发、运维成本高：渠道体系庞大，传统点对点集成链路过多，数据接口格式不一致，导致需要投入大量 IT 资源。

财务结算周期长：存在数据孤岛，财务结算前仍需与渠道商基于各自数据进行人工对账，导致结算周期长。

区块链解决方案

针对上述问题，联想正在尝试使用区块链技术搭建渠道销售数据共享平台。联想渠道商使用统一的 Dapp（Decentralized App 去中心化应用），在发生实际销售行为时，通过扫描产品外包装的序列号信息并填入对应交易数据，通过 Dapp 将数据上传至区块链平台。业务参与方均可以通过区块链平台共享数据查看商品流转信息。联想还可以基于此平台数据进行汇总计算销售 3S，库存等关键指标，指导制定销售计划并进行高效的财务结算。

表 4-2 区块链对渠道销售业务优化

	目前体验	区块链优化后
数据收集方式	多种数据收集方式点对点集成，格式不统一	统一使用 Dapp 进行数据共享区块链平台提供统一接口
数据实时性	手工上传，数据无实时性	业务发生时同步共享数据
数据准确性	需要人工校对数据	合约逻辑控制，增强准确性
数据可信度	中心化、可篡改、难追溯，数据不可信，需要引入对账环节	共识统一分布式账本 数据不可篡改 数据历史全程可追溯

此方案总体借助溯源的思想，为联想的渠道商提供了统一的数据共享方式，统一的数据接口方案，操作方便，可扩展性强，并保证交易数据在业务发生时实时上链共享，提高数据实时性。此方案结合了区块链的数据可追溯性、不可篡改性，用以保证每一件商品在渠道销售全程可追溯，提高数据的准确性，减少后期人工校对数据，同时结合共识特性，保证各节点账本一致性，来减少财务结算前的对账环节。

在技术实现上，此方案也充分利用联想区块链平台隐私保护的特性，对敏感、隐私数据进行加密保护，在实现数据共享，高效协作的同时，保护各参与方隐私安全。

面临的挑战及应对

此方案的实施需要各级渠道商的高度参与，但渠道网络本身非常庞大，项目实施规模过大，因此在实施中，联想采取如下方式：

01

- 优先进行小规模实验：在实验项目开发、测试以及使用过程中，不断听取渠道商的建议和反馈，增强产品的易用性，为后续产品推广夯实基础。

02

- 引入激励机制：联想一直致力于和合作伙伴一起为客户提供优质服务，并帮助合作伙伴取得更大的成功。为此，联想计划将渠道商的参与度指标纳入到联想渠道商评级的考量中，使渠道商享受数据共享带来便利的同时可以获得更多的激励，与联想一同取得成功，实现共赢。

供应链金融

背景介绍

国际贸易的全球化趋势正在催生新的贸易融资模式，供应链金融作为有效的金融运作模式受到全球制造业的关注。随着供应链金融的发展，其在保障企业资金流、提升供应链运行效率方面起到了积极的作用。金融领域作为区块链技术应用落地的重点方向之一，各技术平台和金融机构都对区块链应用进行了积极的探索。联想在供应链金融方向上已经进行广泛的实践，并形成了完整的业务流程。在区块链技术发展的新背景下，相关团队也在逐步利用区块链优化传统供应链金融业务模式。

业务痛点

联想供应链金融为渠道商建立了一套完整的金融解决方案。此方案建立在联想全面的信用管理体系上，在对渠道商及客户进行完备分析后，与商业银行进行保理或保兑融资服务，其中涉及了企业信用评价、账款控制、财务报表等多种信息，引入了包括联想、银行、渠道商、客户等多个企业角色。随着客户的不断增多，业务部门需要处理的信息也在成倍增多，工作强度和难度都在不断增加。

01

- 业务流程链条较长。银行与企业为降低潜在风险，需要签订各类三方协议，由此带来较多的线下文件处理工作，需要保存相应文件作为凭据，而且在尚未实现系统对接时，还需要向银行提供融资相关的交易数据；

02

- 信息传递具有一定的滞后性。现有融资网络中存储的部分信息需要人工维护。同时涉及的行业范围较广，如果某企业在其他银行或商业网络内出现信任问题，相关人员很难在第一时间获取信息；

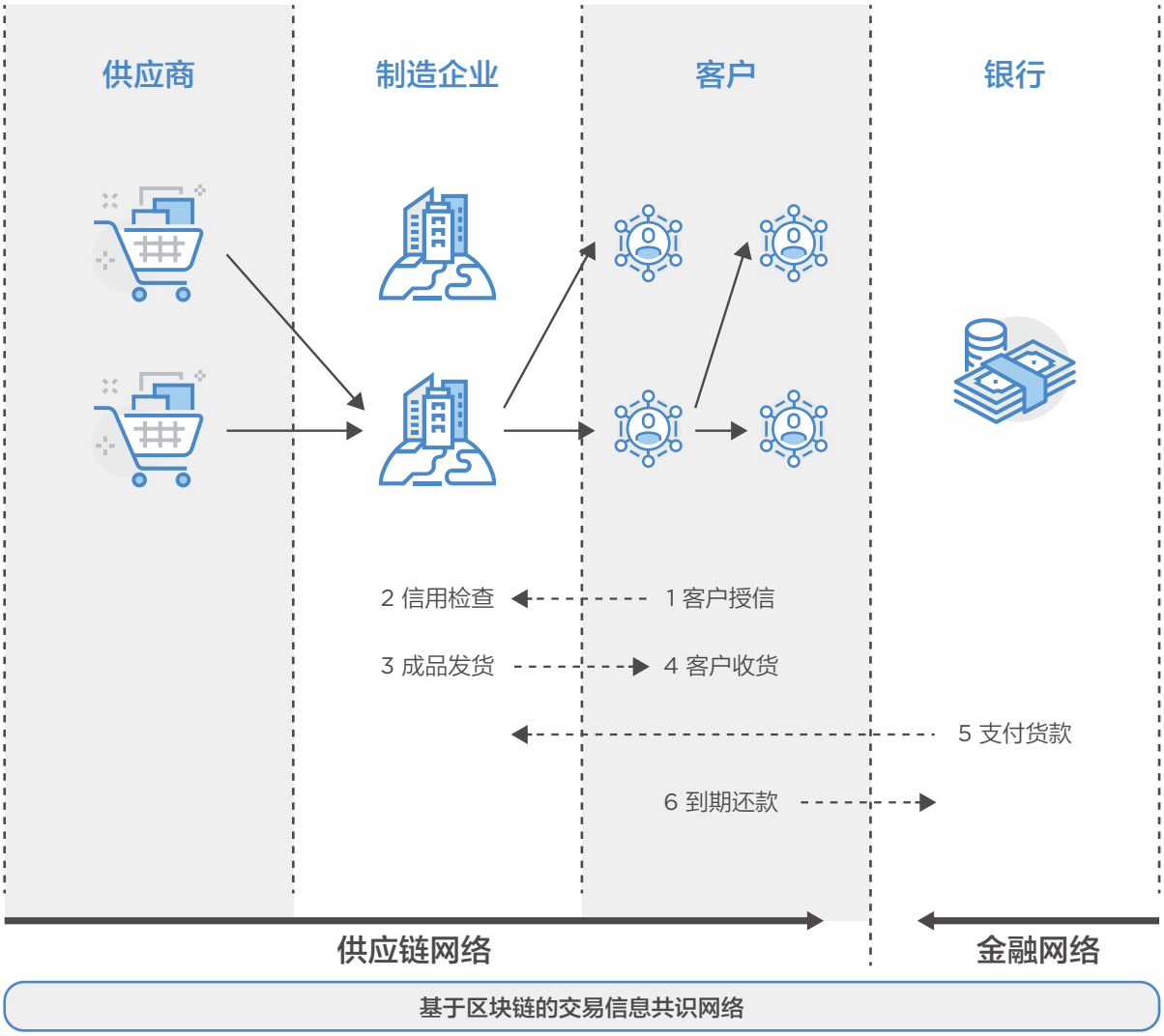
03

- 较高的参与门槛限制了金融服务的范围。建立类似联想的现有金融模式需要满足相应的前提条件，准入企业需要具备较强的技术和经济实力，并且自身也要具有一定的信誉和资源。

解决方案

在区块链技术的支持下，供应链金融企业从业务信息共享和流程处理方式入手对现有业务模式进行调整。

制造企业、渠道和金融机构将现有的第三方融资过程通过区块链进行数据记录。制造企业在对客户进行授信时，同样将授信额度记录在区块链上，银行可以随时查看；渠道在授信范围内完成交易后，可以按照交易额度到银行进行融资，并通过设定智能合约，在制造企业发货后，由银行自动进行付款并为客户计息；渠道在向银行付清欠款后，自动恢复授信额度。同时，类似的融资需求具备向下游渠道进行扩展的能力，下游二级渠道可以将其与一级渠道的交易记录上传去区块链网络，进一步扩大物料转移的账本范围，为更多渠道提供获得融资的可能性。最后，在网络经过充分扩展后并构建全产业生态后，在其他网络内出现问题都可以及时反馈至各参与方，为快速完成信用审核提供依据。



图：基于区块链的供应链金融解决方案

业务变革

区块链技术为供应链金融领域的业务变革提供了一种全新的模式。围绕制造企业建立起来的供应链交易记录，可以作为银行贷款和企业融资的凭证，尤其是面向渠道商、供应商以下的二级和三级业务合作伙伴。这部分渠道商和供应商恰恰是最需要资金支持的中小微企业。通过围绕核心制造企业建立的区块链网络，中小微企业可以利用交易记录向银行申请贷款，从而服务于更多商业客户，形成新型的基于区块链技术的供应链金融商业模式。

技术挑战及应对

金融区块链对于数据的敏感性要求更为迫切，需要具备强于一般交易联盟的加密机制，例如对于智能合约的额外加密保护，防止黑客通过篡改合约内容，窃取数字资产。另一方面，供应链金融融资的依据依然是企业的交易记录，在企业间建立联盟链后，其他网络可以通过跨链集成技术，核对交易记录状态，为更多的金融服务提供背书依据。由此不仅能够提升企业联盟链的应用范围，还可以有效的解决金融企业由于缺少行业背景，很难搭建交易平台的问题。同时，目前主流的隐私保护算法也存在一些性能上的影响。因此，随着区块链网络不断扩展，基于跨链共识、零知识验证以及基于硬件的可信执行环境等关键技术的组合才能最终充分发挥联盟链优势。

区块链助力联想智能化转型战略

区块链对于联想提出的智能化转型战略，将起到相辅相成的作用，是推动战略落地的催化剂。与此同时，联想还将形成应用与技术协同发展的模式，重点围绕全球供应链业务，开展区块链应用的探索和实践工作。

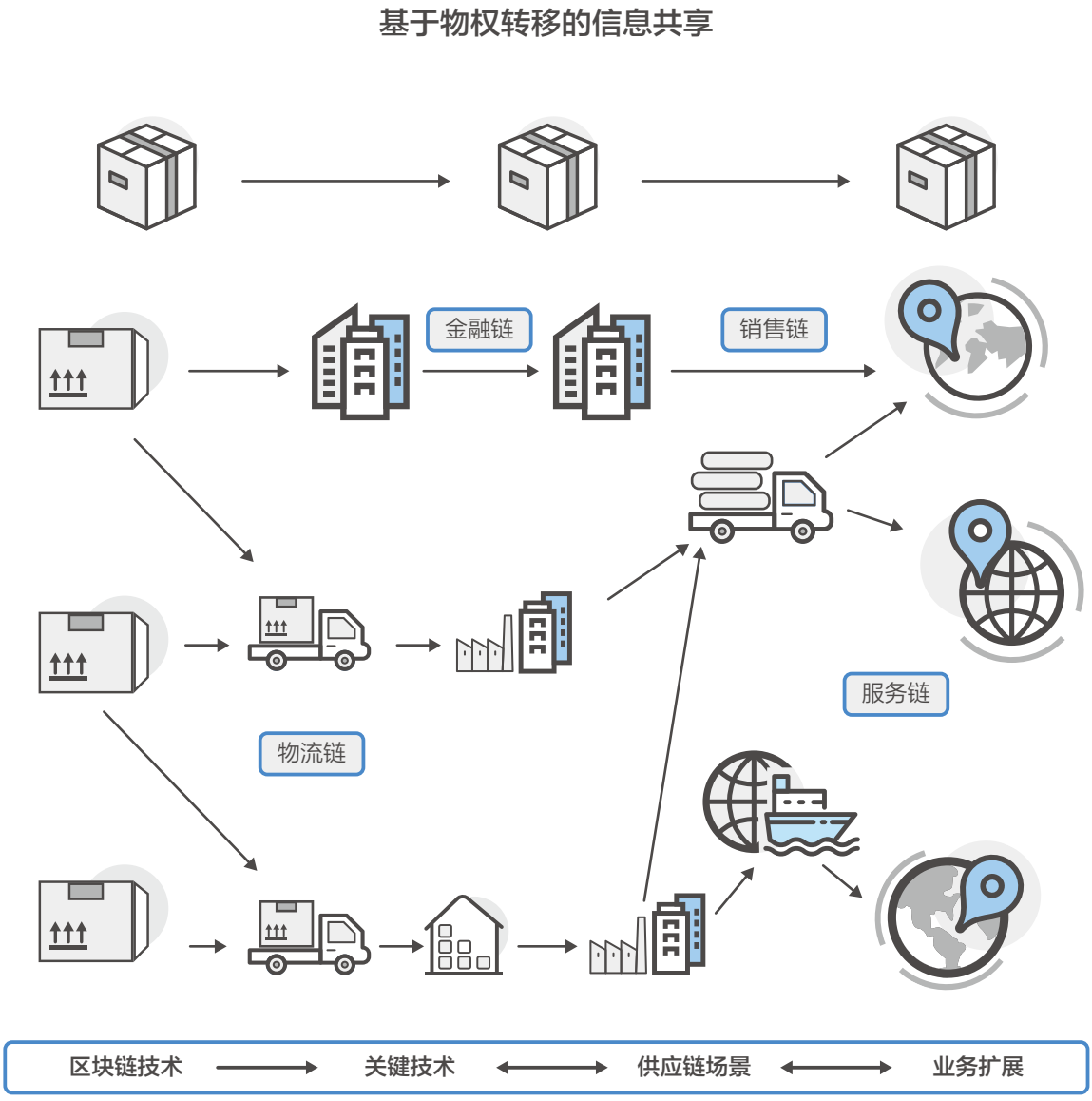
数据是智能化转型的燃料，区块链是放大燃料效能的催化剂

联想在推动整个社会的“智能 +”工程中，提出了助力企业实现智能化转型的发展战略，将在数据、计算力以及算法等领域进行重点布局。区块链技术将对联想的智能化转型战略起到促进作用。

智能化转型战略中明确指出了数据在智能化发展的基础地位，而区块链具备增强数据可信度的特点，能够明确数据的属主，将极大地扩展数据的应用范围与可用性，促使企业数据变现，将现有业务场景中的单一业务数据，变成可以为更多业务服务的共享数据。

围绕全球供应链业务，实现技术与应用的协同发展

通过在全球供应链领域应用区块链技术，联想期望在未来规划一套全新的基于物权转移的供应链运行模式。该模式将供应链中的产品流、信息流和资金流进行高度集成，借助联想在物联网设备、服务器等领域的硬件基础，逐步完成在供应链领域模式转型。在实践过程中，还将重点研究实际业务应用过程中发现的技术问题，弥补区块链技术存在的各类问题，为业务领域的扩展提供技术支持。



图：区块链发展模式方案

如图所示，联想将围绕全球供应链业务，借助数据发展战略的推力，逐步搭建物流链、金融链、销售链与服务链等业务链条，服务实际业务需求。同时，在业务实践过程中，不断扩展业务上下游合作方，不断研究区块链关键技术，促进区块链技术和应用协调、有序、高效的发展。

区块链的愿景

掌握全球科技竞争先机，在前沿领域乘势而上、奋勇争先，在更高层次、更大范围发挥科技创新的引领作用，是坚持建设世界科技强国的奋斗目标。

习主席在报告[1]中提出，要以智能制造为主攻方向推动产业技术变革和优化升级，推动制造业产业模式和企业形态根本性转变，以“鼎新”带动“革故”，以增量带动存量，促进我国产业迈向全球价值链中高端。这也是联想集团坚持创新、立足智能制造、立足供应链创新的原动力。而当前正在飞快地进入到一个全新的时代，由人工智能驱动的智能化变革正地向我们走来，正在引发第四次工业革命。

联想认为，人工智能，更准确说增强智能（Augmented Intelligence）发展的三大要素是，数据、计算力、算法，正是因为这三个要素在过去数年的高速发展，才让智能化走得越来越快，离我们越来越近。

区块链作为颠覆性新技术，是联想在供应链领域改造的核心技术，更是联想坚持用 AI 赋能各行业的关键保障，必会在创新的科技舞台上呈现浓墨重彩的一笔。

技术趋势

安全技术是区块链构建中最重要基础，区块链的实施方案包含基础设施，平台，应用三层，会以软件 + 硬件相配合的方式，构建高度可信可靠的安全能力。其中区块链自身的技术强化将成为近期关注对象，而区块链系统异构融合的演变以及和人工智能、物联网的结合将成为未来区块链技术的主要趋势。

区块链技术强化

逐渐成熟的区块链技术，在商业实施中已经遇到包括算法安全性、协议安全性、使用安全性、实现安全性和系统安全性的挑战。因此，加强对加密技术、密钥存储、隐私保护、共识协议等技术实现等方面的安全研究，提高区块链技术的整体安全可靠水平，势必是区块链技术在未来发展的首要一步。

区块链系统异构融合

去中心化是区块链技术的基础。传统的系统架构多是单一中心模式。借助区块链技术，参与者可以在无中心节点的架构中直接建立多方协同合作的平台，每一方都留有全部相同的协作信息，此种新架构改造了原有的中心模式。简化的交易流程将会降低交易成本，多方同时参与的新合作模式将会提高信息信任的传递效率。随着技术的逐步演变，新形成的这些离散的区块链系统还会逐渐融合，最终形成由多个区块链网络相互对接，链内自治、链间合作的多链和跨链模式。

区块链与人工智能

充分做到隐私保护并且实现价值的全流程可追溯是区块链技术的关键特性。这恰好解决了人工智能数据需要保护的需求。人工智能技术需要依托数据生成模型，并通过不断训练生成新的数据进行优化完善，大量信息数据的隐私性对于参与方尤为重要，而区块链技术可以利用其隐私保护的特性将这些数据进行加密，充分保证了数据的安全性。而借助区块链系统实现了训练全过程的透明化和可追溯，对于各参与方的数据变现和确保收益提供了最终的保障。

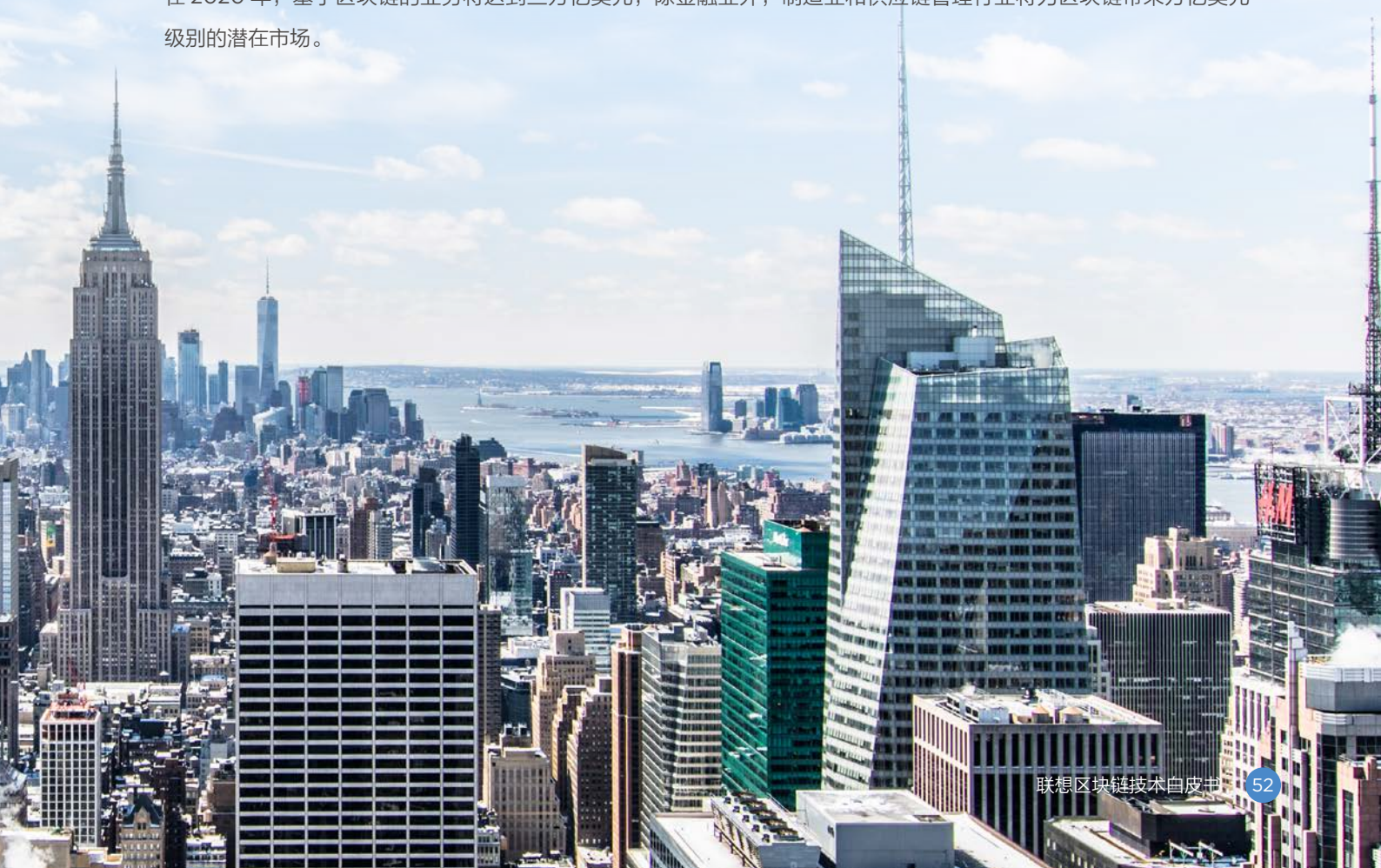
区块链与物联网

分布式和自组织作为区块链技术的另一个特点，与传统物联网的分布式网络具有极大的相似性。在物联网当中对于每一台设备、每一个环节的管理与控制显然需要大规模的物理依赖，据预测，全球的物联网设备数量将在 2020 年达到 250 亿台左右，设备的建设和维护费用将是一笔不小的开支。区块链技术的分布式结构以及共识机制的介入将会改善物联网模式，简化流程，优化链路，实现分布式物联网的去中心化控制，同时物联网中包含大量的数据，通过区块链技术，也可以使得这些数据进行变现。并且，现阶段的网络都是尽力服务（best effort）模式，如果有了区块链的点对点支付，将重构物联网的服务结构，使之更高效。

应用趋势

区块链技术从比特币应用的爆发期，演变到各行各业跃跃欲试并大力发展，经历了从野蛮生长到高速发展的过渡阶段。

达沃斯论坛创始人克劳斯 • 施瓦布（Klaus Schwab）认为，区块链作为继蒸汽机、电气化、计算机之后的第四次工业革命的重要成果，预计到 2025 年之前，全球 GDP 总量的 10% 将利用区块链技术储存。市场研究机构 Gartner 预测，在 2020 年，基于区块链的业务将达到三万亿美元，除金融业外，制造业和供应链管理行业将为区块链带来万亿美元级别的潜在市场。



智能合约的普及化

智能合约不仅会用于有形资产的所有权、转让权的确认，同时也会用于无形资产的保证，例如知识产权的保护、网络域名的管理等。而且，智能合约作为一种新型的可以避免篡改、抵赖和违约的合约，将适用于所有契约性的约定中，保障所有合约的可靠性。

应用模式改变

公有链的安全性问题是人们广泛关注的问题之一，与日俱增的交易量以及公有链的性能缺陷不可调和。因此，未来的区块链应用将趋于采用联盟链、公有链、私有链等多链混合使用、各区块链系统自组织并相互融合的模式。此模式不仅对技术而言是挑战，而对上层应用而言也是模式的根本改变。

应用领域扩展

虽然本白皮书中已经总结了一些新兴应用领域，但是这是远远不够的。随着政府部门不断出台的技术标准和政策，以及应用普及和社会认知度的提高，区块链技术将逐渐向社会各领域渗透，并成为社会应用领域的常态。例如，区块链已经初步的应用于金融、供应链、公益、文化娱乐、教育等领域。

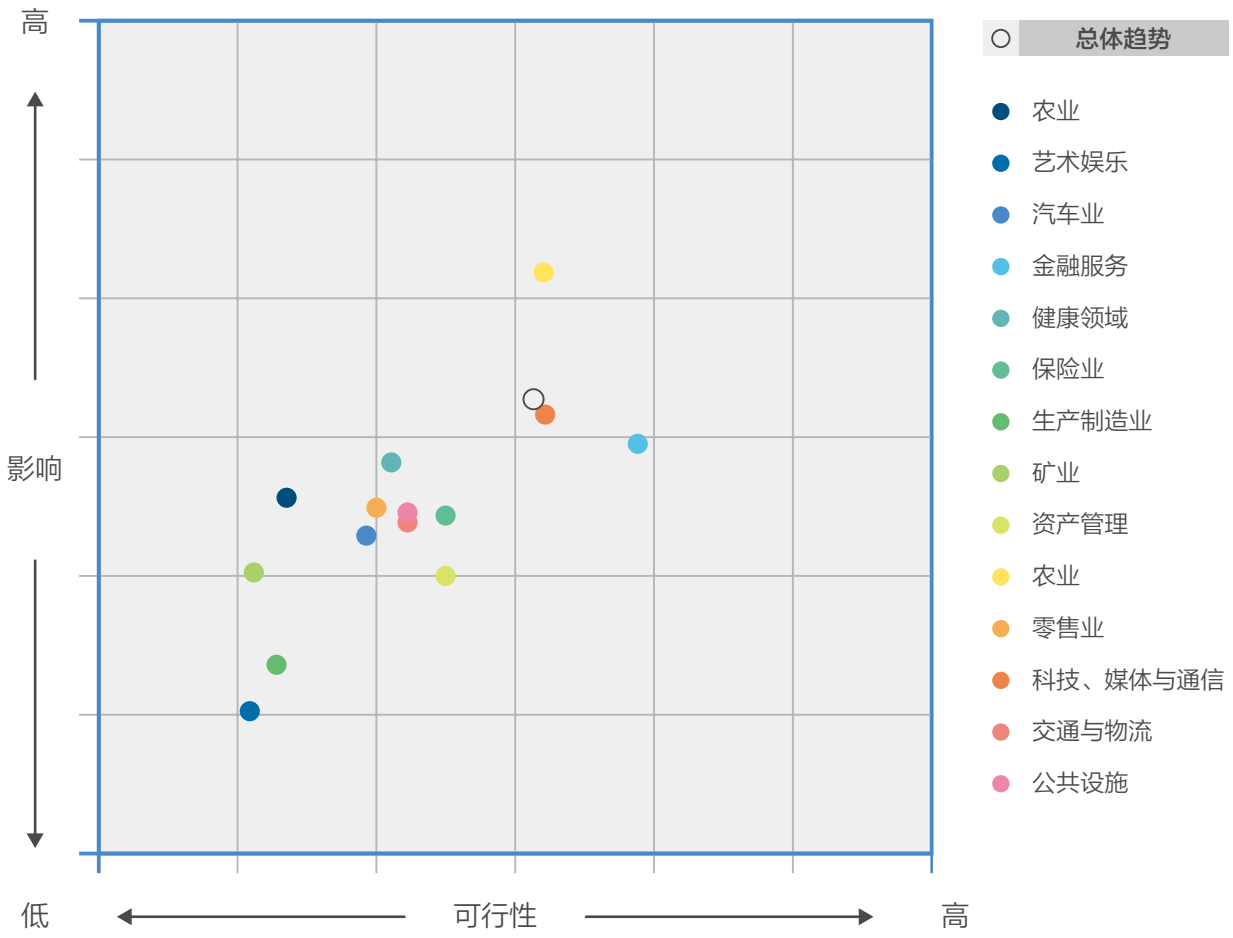


图 5-1 区块链行业领域分布 [37]

行业赛道格局形成

随着越来越多的企业尝试区块链应用，每个行业中都会逐渐产生领头的先锋队伍“企业作为创新的主体，是推动创新创造的生力军。”[1]，他们汲取自己最擅长的部分用来实例验证，形成有效场景。最终从百花齐放的尝试阶段进而发展出成熟的商用案例。同时通过领头军探索开展的区块链应用试点示范工作，推动区块链技术和行业应用的融合发展，逐步把应用扩展到各行各业。

社会责任

企业在大力发展新兴技术，落地商业场景的同时，也需要关注人的因素。关注人，关注社会，改善现状，为周围世界带来更积极的影响，是企业以人为本的社会责任之一。

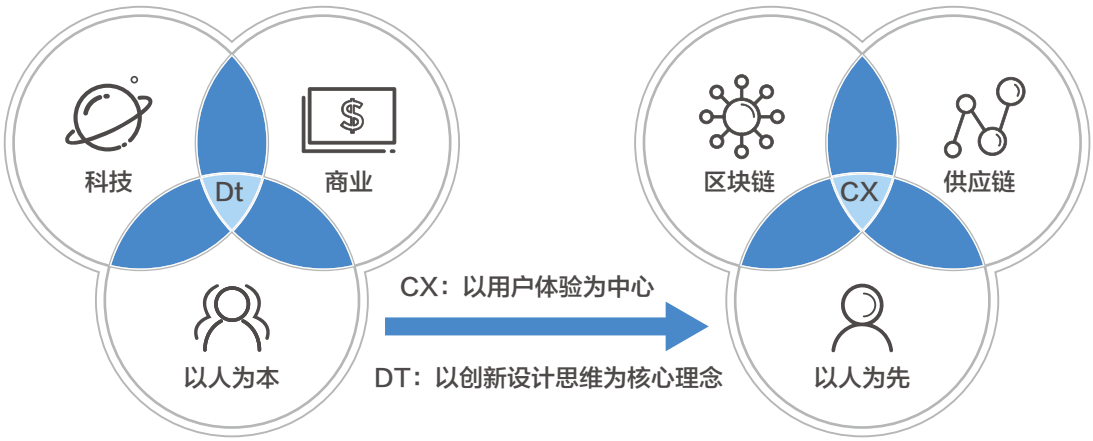


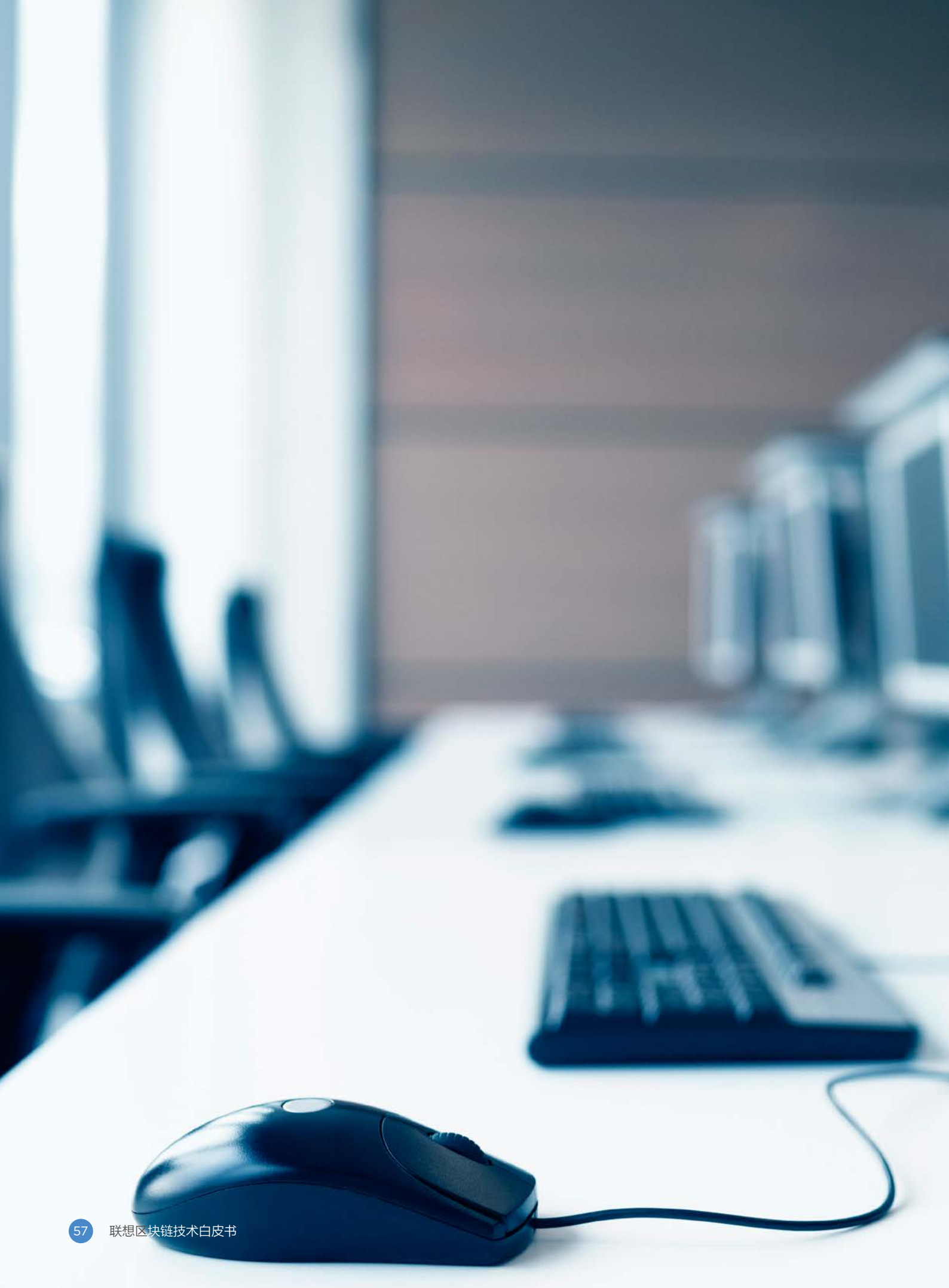
图 5-2 创新设计思维在区块链项目的运用

特别是对于体量大的企业来说，日常业务所涉及的领域广，在验证及应用新技术的方面具有先发优势，因此，身先士卒，勇于示范，乐于分享，积极运用创新思维，不断探索新技术新领域，也是企业创新挑战的一份社会责任。

联想作为百万级应用企业，放眼大处，着手小处，快速行动。饯行创新设计思维模式，面对新技术保持高效性和敏感性。在行业内作为领头羊、先驱者，率先对新兴技术积极研究，并以日常供应链业务作为契机，对各个场景进行验证，推演，试验，探索了一套崭新的业务模式。

在企业示范作用的同时，联想将创新精神融入到日常业务细节，建立了跨部门协作的区块链项目虚拟团队 ---LeChain，将及时把握行业动态，随时攻克技术难点，密切关注项目需求，时刻追踪项目进程各节点串联成环。能够从市场洞察、内部管理、技术平台开发等多个角度给出专业性意见，并能够就项目关键问题迅速形成共识。以小团队，大职能，行动迅速的特点，最大程度的将以用户为中心，创新实践，快速迭代的模式推动了区块链技术发展。

在整个区块链技术的实施与验证过程中，企业会在寻找新技术的可行性，商业的可能性以及人的需求期望值，三方面充分连接真正形成了以用户中心的优质企业。充分将三者完美结合，客户在新的场景下会拥有更好的体验。在未来不断尝试的过程中，期待越来越多的企业会秉承不断创新、不断挑战，以人为本的精神，为世界更加美好贡献力量。



参考文献

[1]《习近平：在中国科学院第十九次院士大会、中国工程院第十四次院士大会上的讲话》http://www.cac.gov.cn/2018-05/29/c_1122901495.htm

[2] Diffie W.,New direction in cryptography[J].IEEE Trans.inform.theory,1976,22.

[3] Nakamoto S.Bitcoin:A peer-to-peer electronic cash system[J].Consulted,2008.

[4] Boyd S,Ghosh A,Prabhakar B,et al.Randomized gossip algorithms[J].IEEE Transactions on Information Theory,2006,52(6):2508-2530.

[5] DagCoin:acryptocurrency withoutblocks

[6] https://bitslog.wordpress.com/2015/09/11/dagcoin/

[7] Nair D T,Johnson R E,Prakash S,et al.Replication by human DNA polymerase-iota occurs by Hoogsteen base-pairing.[J].Nature,2004,430(6997):377-80.

[8] Anton Churyumov.Byteball:A Decentralized System for Storage and Transfer of Value.

[9] Nikolay N,Marin I,Doncho K,Simeon K.The Fabric Token(FT)Ecosystem High-Level Development& Management of Smart

[10] https://ziggurat.cn/

[11] [33]https://baijiahao.baidu.com/s?id=1605683467436674708

[12] 华为：《华为区块链白皮书——构建可信社会，推进行业数字化》

[13] 京东：《区块链技术实践白皮书》

[14] 腾讯：《腾讯云区块链 TBaaS——产品白皮书》

[15] 麦肯锡：《区块链——银行业游戏规则的颠覆者》

[16] 袁勇 , 王飞跃 . 区块链技术发展现状与展望 [J]. 自动化学报

[17] 林小驰 , 胡叶倩雯 . 关于区块链技术的研究综述 [J]. 金融市场研究 ,2016(2):97-109.

[18] 梁秀波 , 李启雷 , 尹可挺 , 等 . 一种基于加法同态加密的区块链隐私保护方法 :,CN106549749A[P].2017.

[19] 祝烈煌 , 高峰 , 沈蒙 , 等 . 区块链隐私保护研究综述 [J]. 计算机研究与发展 ,2017,54(10):2170-2186.

[20] KUZMIN A.Blockchain-based structures for a secure and operate IoT[C]//IEEE Internet of Things Business Models,Users,and Networks.2018.

[21] ZHI Q H,XIONG Y S,YAN X Z,et al.A decentralized solution for IoT data trusted exchange based-on Blockchain[J].IEEE International Conference on Computer and Communications,2017(3):1180-1184.

[22] YANG C,CHEN X,XIANG Y.Blockchain-basedpublicly verifiable data deletion scheme for cloud storage[J].Journal of Network&Computer Applications,2018,103-112.

[23] NOVO O.Blockchain meets IoT:an architecture for scalable access management in IoT[J].

[24] IEEE Internet of Things Journal,2018(3):1184-1195.

[25] Camenisch J,Dubovitskaya M,Lehmann A,et al.Concepts and Languages for Privacy-Preserving Attribute-Based Authentication[M]//Policies and Research in Identity Management.Springer Berlin Heidelberg,2013:25-44.

[26] Jin H,Dai X,Xiao J.Towards a Novel Architecture for Enabling Interoperability amongst

[27] Multiple Blockchains[C]//IEEE,International Conference on Distributed Computing Systems.IEEE Computer Society,2018:1203-1211.

[28] Miller D.Blockchain and the Internet of Things in the Industrial Sector[J].It Professional,2018,20(3):15-18

[29] Henry R,Herzberg A,Kate A.Blockchain Access Privacy:Challenges and Directions[J].IEEE Security& Privacy,2018,16(4):38-45.

[30] Aste T,Tasca P,Matteo T D.Blockchain Technologies:The Foreseeable Impact on Society and Industry[J].Computer,2017,50(9):18-28.

[31] Aniello L,Baldoni R,Gaetani E,et al.A Prototype Evaluation of a Tamper-Resistant High Performance Blockchain-Based Transaction Log for a Distributed Database[C]//Dependable Computing Conference. IEEE,2017:151-154..

[32] https://www.hyperledger.org/announcements/2016/02/09/linux-foundations-hyperledger-project-announces-30-founding-members-and-code-proposals-to-advance-blockchain-technology

[33] 工信部：《中国区块链技术和应用发展白皮书（2016）》

[34] UK GovernmentOffice for Science,Distributed Ledger Technology:beyond block chain.January 2016. Retrieved 29 August 2016.

[35] 最高法院：《最高人民法院关于互联网法院审理案件若干问题的规定》

[36] 欧盟：《通用数据保护条例 GDPR,General Data Protection Regulation》

[37] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value?cid=eml-web

术语解释

- **Channel（通道）：** 通道是构建在超级账本 Fabric 系统上的区块链账本数据，实现了数据的隔离和保密。通道特定的账本在通道中是与所有对等节点共享的，并且交易方必须通过该通道的正确验证才能与账本进行交互。通道是由一个“配置块”来定义的。

- **Anchor Peer（锚节点）：** 锚节点是通道中能被所有对等节点探测、并能与之进行通信的一种对等节点。通道中的每个成员都有一个(或多个，以防单点故障)锚节点，允许属于不同成员身份的节点来发现通道中存在的其它节点。

- **Block（区块）：** 区块由区块头和区块体组成。区块体中包括一组有序的交易通过哈希算法形成默克尔树根存储在区块头中。区块是一组有序的交易集合，在通道中经过加密（哈希加密）后与前序区块连接。

- **Endorsement（背书）：** 背书是指一个 peer 节点执行一个交易并返回 YES/NO 给生成交易提案的客户端的过程。

- **Endorsementpolicy（背书策略）：** 节点通过背书策略用来确定一个交易是否被正确背书。当一个 peer 节点接收一个交易后，就会调用与该交易相关的 Chaincode 作为交易验证流程的一部分来确定交易的有效性。背书策略定义了依赖于特定链码执行交易通道上的 peer 节点响应结果的必要组合条件（即返回 Yes 或 No 的条件）。

- **Chaincode（链码）：** 链码是一段程序，用来处理一些得到各方共识的业务逻辑，链码的编写可实现 Fabric 提供的一套接口，并需要运行在一个安全的 Docker 容器中。链码具有相应的背书策略，其中指指定了背书节点。

- Consensus（共识）：共识是保证每一笔交易在所有记账节点上记账的一致性，其用于产生一个对于排序的同意书和确认构成区块的交易集的正确性。

- **Token（“令牌”/“通证”）：** Token 本是一个计算机安全术语，是计算机身份认证中“令牌” 的意思。在数字经济的语境中，Token 类似于区块链生态里用于流通的货币，也就是代币。比如，我们平时所说的比特币、以太坊就是 Token。虽然被称为代币，也类似于货币，但是从 Token 这个词的本义以及具体内容来看，其本质上是一段代码，并不是货币。

- **Public Blockchain（公有链）：** 公有的区块链，读写权限对所有人开放。公有链的典型代表是比特币和以太坊。公有链的验证节点遍布于世界各地，所有人共同参与记账、维护区块链上的所有交易数据。

- **Private Blockchain（私有链）：** 私有的区块链，读写权限对某个节点控制。私有链的读写权限掌握在某个组织或机构手里，由该组织根据自身需求决定区块链链的公开程度；适用于数据管理、审计等金融场景。

- **Consortium Blockchain（联盟链）：** 联盟区块链，读写权限对加入联盟的节点开放。典型代表是超级账本（Hyperledger）。超级账本基于透明和去中心化的分布式账本技术，联盟内成员共同合作，通过创建分布式账本的公开标准，实现价值交换，十分适合应用于金融行业，以及能源、保险、物联网等其他行业。

Lenovo 联想

800-900-1569
400-898-1569
HTTP://B2B.LENOVE.COM.CN