京东

京东区块链
技术白皮书

·2018年3月·

序

区块链技术推动价值大数据的高效、可信流动

“技术引领，正道成功”！

这是京东集团董事局主席刘强东先生在 2017 年 618 购物节期间，对外界正式发布的京东未来发展战略。在过去的十四年中，京东用了很长的时间证明自己是一家成功的零售公司；现在，京东正在用实践证明自己也是一家领先的技术公司。京东集团正在全面迈向技术转型，引领第四次零售革命的全面升级。京东对于技术领域的投入，尤其是针对 AI（人工智能），Big Data（大数据），Cloud（云计算）等新兴领域的投入，加速了京东向全社会提供“零售即服务 ‘Retail as a Service, RaaS’ ”的零售基础设施服务的步伐。

区块链作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用，在京东所在的零售领域有着非常多的结合场景。尤其是其去中心化以及新型信用体系的建立方式，对于京东在技术转型方面的战略愿景，以及在消费者心中长期所建立起来的正道形象非常匹配。目前，区块链的发展势头，将在技术领域成为云计算、大数据、及人工智能之后，并列于移动互联网从中心到边缘、5G 物联网等新一代信息技术，共同引发并推动新一轮的技术创新和产业变革。

为推动区块链技术的发展和京东集团各种业务场景的结合，运用区块链技术推动价值大数据的记录、流动和交换，京东集团联合了内部各职能、技术、及业务体系，开展区块链技术和应用发展趋势专题研究，编撰形成了《京东区块链技术白皮书（2018）》。白皮书总结了区块链核心关键技术在京东集团的发展现状和方向，分享了京东集团各个业务落地实践的典型应用案例，为业界区块链技术发展路线图和标准化路线图提出了相关建议。白皮书内容详实、分析透彻，落地场景扎实，具有相当好的参考价值。在发布白皮书的同时，我们期待与业界有识之士共同努力，积极把握区块链发展趋势和规律，营造良好正道的技术发展环境，

加速推动区块链技术的发展和各种应用场景的落地结合。

京东集团首席技术官

张晨

前言

区块链技术将引领互联网数据存储与交换的巨变，开启信任经济时代。

自去年开始，区块链技术独立于比特币，逐渐进入科技公司和人民群众的视野，引发了广泛关注与大量讨论。学术界和工业界普遍认为区块链技术是下一代数字经济的基石，可以极大的推动数据的可信存储、商业协同、数据可信的交换和分享，以及随之诞生的新兴商业模式。

伴随着每一家公司对于区块链技术的追逐和不懈探索，我们也留意到一些过热的泡沫和技术噱头的杂音，同时现有区块链的开源平台也暴露出读写性能、模块标准化、应用灵活支持、监管和法律认可、安全和隐私保护等多个方面亟待改善之处。除此之外，区块链领域的人才稀缺也极大抑制着我们对于这项技术的规模化应用。

京东集团拥有全渠道零售和端到端供应链的高质量大数据，区块链技术天然可以解决京东业务场景中多个主体的信息记录与分享，可信数据交换与传递的业务诉求。早在 2016 年，京东集团就全面启动了区块链技术在京东业务场景中的应用探索与研发实践，先后在数据交易、供应链管理、金融科技等领域落地了不同的区块链应用，过程中积累了大量的区块链部署经验与底层技术研发能力。

历经几年时间的应用和探索，京东认为区块链技术在以下三个方向存在巨大的应用机会，引领数字经济的变革——

- **建立社会化共享的可信数据库**

  区块链的技术本质是一种去中心化、面向业务、跨主体、健壮与安全的分布式状态机。其本身的存储数据、共有数据、分布式、防篡改与保护隐私、数字化合约等 5 项核心特征。基于这些特征，部署跨主体间的区块链联盟链节点和桥接，用区块链技术搭建一张社会化的共享数据存储网络，有机会以客观的技术手段来解决跨主体

的信任问题。

- **提升交易效率，降低交易成本**

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

- **推动供应链创新**

  伴随着中国政府将供应链创新与应用上升为国家战略和居民消费的不断升级，供应链风险控制和供应链透明度提升的诉求不断攀升。区块链技术可以搭建供应链全流程节点共同维护的联盟链，在联盟链中建立数据维护的参与规则与激励机制，鼓励供应链节点中的企业参与和维护供应链数据，促进供应链数据的协同和互通，进而提升整条供应链的透明度，同时也可为消费者购买商品的溯源和防伪提供技术支持。

京东在区块链技术的创新与实践过程中，逐渐认知到区块链并不单纯是一种技术，而是一种社会化的“共识信任”理念，这种理念鼓励人们在互联网中建立一套可以被监督并且拥有治理规则的系统，而推广这一社会化理念不能依靠一家之力，而需要协同盟友共赢未来。我们积极拥抱区块链技术带来的变革，同时也期待将我们实践和应用区块链技术的经验分享出来，与合作伙伴一同解决区块链应用和推广中仍未解决的问题，基于以上，京东集团组织和编写《京东区块链技术白皮书》。不同于区块链研究领域内的其它白皮书，这份白皮书没有过多阐述区块链技术的宏观环境和解决方案，而是立足于区块链技术平台本身，以一个实践者的角度，结合京东潜在的区块链应用场景，给出区块链技术研发和应用的建议和经验分享，期待携手合作伙伴共建区块链技术生态，落地更多的区块链“杀手级”应用。京东正在

积极筹备开放支撑自身落地应用的区块链 BaaS 平台，帮助政府、物流商、品牌商、金融机构等合作伙伴组件适用的区块链技术平台，伴随着 BaaS 平台的开放和技术应用的不断积累，京东区块链技术团队将持续更新这份白皮书，以便补足现在版本中未涉及或存在缺陷的部分。同时，京东集团各技术、业务部门也会针对自身的应用场景和实践经验，陆续对区块链技术进行垂直领域的深入解读。

京东的目标是以区块链为“链接器”，结合自身在云计算、大数据、人工智能、物联网等新技术上积累的经验，构建一体化的智慧供应链体系、零售网络和金融科技，拉近商品与客户的距离，在无界零售的集团战略指引下，全面开放自身的区块链技术积累，与您共赢未来！

欢迎各界合作伙伴来信交流指正！

y@jd.com

2018 年 03 月

编委会成员

顾问：

张晨 裴健 于永利 杨海明

主要作者：

林世洪 孙海波 黄海泉 王义 张伟 仉良 朴成林 张作义 迟楠 刘文婧 周晓健 翟欣磊

视觉设计:

崔伟

目录

加我聊聊

新科技领域 战略性新兴产业

PreIPO 项目 独角兽项目

私募股权投资基金

欢迎各**城市财富管理机构**联系我

欢迎各**上市公司、大企业投资部门**联系我

欢迎对**私募基金**有兴趣的朋友联系我

1. 区块链技术简介

上世纪 70 年代以来，随着密码学技术、分布式网络、共识算法以及硬件存储计算能力的飞速发展，通过技术手段实现多主体间共识机制建立的条件日趋成熟，为解决多主体环境下的中介机构信任风险、降低交易成本、提升协同效率提供了全新的解决思路。

中本聪于 2008 年发表了名为《比特币：一种点对点式的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）的论文，详细描述了如何创建一套去中心化的电子交易体系。这种体系不需要创建在交易双方相互信任的基础之上，首次通过技术手段实现了交易主体间共识机制的建立，而“区块链”技术正是构成这种电子交易体系的基础技术。

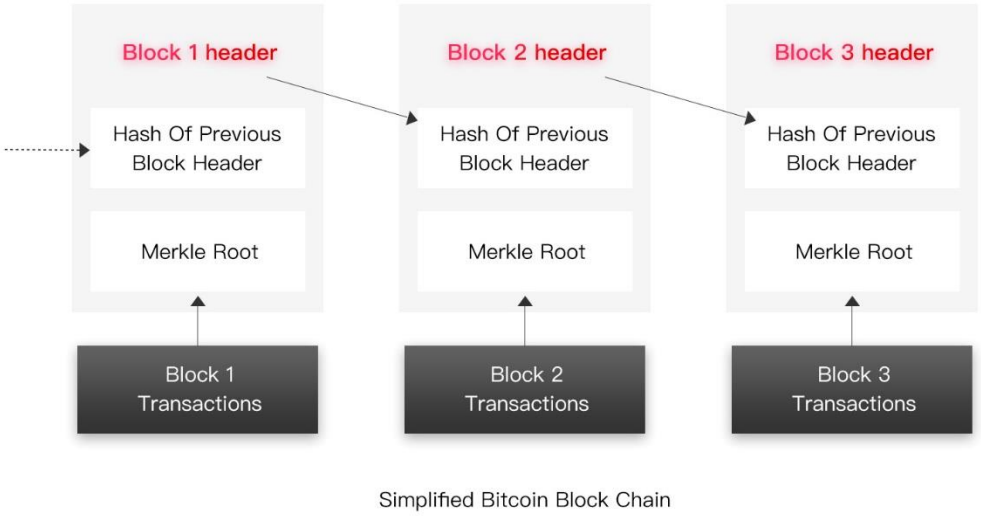

图 比特币工作原理示意

以太坊（Ethereum）是继比特币之后的又一个开创性的区块链项目，于 2013 年末发布白皮书。以太坊开创性地将智能合约（Smart Contracts）和区块链结合起来，在交易主体间共识机制建立的基础上，通过自动触发可执行的电子合约，解决了交易主体间承诺履行

的问题，有效推动了区块链产业化应用的进一步发展。

近年来，区块链技术的不断发展和随之而来的数字货币热潮，引发了从极客到 IT 技术圈、金融领域、产业经济、政府和公共组织、媒体舆论等的广泛关注，围绕区块链技术研究、产业化应用、政策监管等开展了广泛而有益地探索实践。区块链技术的成熟应用尚需时日，但它所带来的多主体共识协同机制的思想，将对社会治理和商业运作产生深刻的影响。

1.1. 什么是区块链

区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来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。简单来讲，在区块链系统中，每过一段时间，各参与主体产生的交易数据会被打包成一个数据区块，数据区块按照时间顺序依次排列，形成数据区块的链条，各参与主体拥有同样的数据链条，且无法单方面篡改，任何信息的修改只有经过约定比例的主体同意方可进行，并且只能添加新的信息，无法删除或修改旧的信息，从而实现多主体间的信息共享和一致决策，，确保各主体身份和主体间交易信息的不可篡改、公开透明。

区块链发展到今天，已经涌现出许多形形色色的区块链项目，我们梳理了这些区块链项目在技术上的共性：**区块**、**账户**、**共识**、**智能合约**这 4 个主要部分构成了目前的区块链系统的通用模型。

- 通过链式结构记录变更历史，这部分被称为**“区块”**
- 通过非对称密钥对表示参与者身份，以某种形式的状态数据库记录当前的信息，这部分被称为**“账户”***(注：以太坊、Fabric 为代表的是账户模型，而比特币是 UTXO 模型)*
- 通过链上编码定义参与者之间的承诺，这部分被称为**“智能合约”**

- 通过某种算法在多节点之间达成状态一致，这个过程被称为“**共识**”

1.2. 区块链有哪些特点

从技术构成的角度来观察区块链有助于我们揭开它的神秘面纱，实事求是地分析区块链，并揭示它的本质特点，理解其价值发挥的内在逻辑。如前所述，区块链并不是一个全新的技术，而是结合了多种现有技术进行的组合式创新，是一种新形式的分布式加密存储系统。

区块链本质上是一种健壮和安全的分布式状态机，典型的技术构成包括共识算法、P2P 通讯、密码学、数据库技术和虚拟机。这也构成了区块链必不可少的 5 项核心能力：

存储数据——源自数据库技术和硬件存储计算能力的发展，随着时间的累积，区块链的大小也在持续上升，成熟的硬件存储计算能力，便得多主体间同时大量存储相同数据成为可能

共有数据——源自共识算法，参与区块链的各个主体通过约定的决策机制自动达成共识，共享同一份可信的数据账本

分布式——源自 P2P 通讯技术，实现各主体间点对点的信息传输

防篡改与保护隐私——源自密码学运用，通过公钥私钥、哈希算法等密码学工具，确保各主体身份和共有信息的安全

数字化合约——源自虚拟机技术，将生成的跨主体的数字化智能合约写入区块链系统，通过预设的触发条件，驱动数字合约的执行

1.3. 区块链适合解决哪些问题

我们通过对比分析、研究国内外各领域的典型应用案例及相关参考文献，并结合自身研发和应用实践，获得了一些有助于在业务中推广应用区块链的经验，并推荐以下特点的应用场景或问题，应该积极考虑尝试区块链技术：

1、 **业务开展需要进行跨主体协作**

当需要为开展跨主体的业务建设 IT 系统时，传统的解决方案通常是两种思路。要么建立和运营一个中心化的系统来处理各个参与方的业务需求，业务数据由中心化的组织维护；要么采用 SOA 架构，由各个参与方发布服务接口，并相互调用，数据仍然维护在各个参与方。如果采用中心化的方案，若是业务的参与方之间是相对独立平等的，要开发建设一个中心化系统是很困难的，包括协调、立项、成本分摊等问题。如果采用 SOA 的方案，则技术实践上比较复杂，技术方案缺少通用性，难以支持复杂的业务。此外，从数据的角度来看，无论是中心化的方案还是 SOA，都难以实现数据防篡改。

在业务参与方之间相对独立平等的跨主体业务协作的场景下，利用区块链的共有数据、防篡改、分布式和数字化合约的特点，能够把一些以往需要在业务层面协调解决的问题，放到技术层面来解决,使得问题的解决过程更高效、灵活以及更具客观性。

2、 **业务开展需要参与方之间建立低成本信任**

大多数业务开展都需要建立一定的信任基础，尤其是跨主体的场景下。对信任建立困难、信任维护成本高的应用场景，区块链可以提供非常有效帮助。

我们从三个方面来考察区块链如何建立低成本信任：

a）数据可信

传统的解决方案中，数据通常是以中心化的方式存储，本应共有的业务数据通常却被强势的参与方持有。这种模式下，数据的可信度是由数据持有者的商业/社会信用来保证的，只能建立主观的可信，对于一些重要的领域，仍需要付出额外的成本来防范数据被恶意篡改的风险。

区块链的解决方案是结合了密码学哈希和数字签名，以区块链条的形式将数据的变更历史按时间先后链在一起，并通过共识协议使得参与的各方都共同拥有这些数据。

由于多方分别持有相同的数据副本，并且数据被签名确认，并记录数据的“指纹”（哈希值），以密码技术保证了数据无法被篡改，数据因此变得可信。

区块链使数据持有变得去中心化，以技术手段实现数据客观“可信”。

b) 合约履行

通常的合约（或者契约、协定、合同）的履行从根本上是由法律来保障的。合约被自觉履行一般都是因为有利益、道德或法律后果，受许多主观因素影响。商业活动中为了防止违约、或对违约进行追索，需要付出高昂的成本（担保、保险、律师费、漫长司法程序等等）。

区块链智能合约的本质是一套数字化形式的契约，由计算机确保严格执行。执行方式上，通常的合约是事后以人的主观意愿来执行；而智能合约是在触发条件被满足后，由计算机程序来保证合约及时地执行，具有客观性。

我们把资产数字化到区块链或与区块链锚定，采用智能合约来描述对资产关系的承诺，同时智能合约的执行过程和结果被区块链严格记录，这样便可以降低履约成本和确保高效履约。

区块链智能合约带来的是“契约”的一种新的更精确的表示形式，以及一种更客观、更严格的执行方式。由于契约是我们社会活动的基础，因此这种变化将会带来更广泛的社会影响。

c) 历史可证明

区块链固化了交易历史，并提供对交易历史的追溯查询，保证交易的不可篡改和不可抵赖。

如果某个事件发生时，这个事件连同时间戳一起被记录到区块链中，将来就可以通过区块链证明这件事确实在这个时间发生过。因此区块链为参与交易的各方保留了可信的历史记录。

3、 **业务过程存在长交易、长周期链条**

业务在多主体间流转时，难以确定间接主体的真实性和有效性，同时由于多主体间的业务隔离，难以延伸出多级业务。

区块链从技术上保证整个长交易、长周期链条的各参与主体身份真实，数据可信，实现信用的多级传递，促进业务链条扁平化，提升业务效率。

比特币作为区块链技术的一种典型应用，在交易市场上市值已达千亿美元，这样的一个高市值系统却是以开源的方式在公共网络上运行了多年，表现出了良好的安全性和健壮性。比特币系统的表现揭示了一个重要事实——以客观区块链技术为手段可以直接建立信任，而不需中介背书。

如果我们把区块链技术推广运用到更广泛的产业、金融、公共服务等场景，将使社会的生产分工方式产生巨大变化，这些变化包括：

- 商业交易过程更容易达成信任，从而降低风险，使交易更具确定性
- 商业交易中间环节被缩减，多方交易可直接达成
- 传统中介的中心化的服务模式将发生巨变

这种影响目前已经逐渐显现，随着区块链的逐渐成熟和应用的不断丰富，这种影响力将会像蝴蝶效应一般逐步放大和深入到整个社会，推动去中心化或多中心化主体间的高效协同和共识决策。人类因掌握“工具”而发展文明，我们相信区块链是一种新的“工具”，最终将促进人类社会的进步发展。

1.4. 区块链发展面临的挑战

目前人们已经广泛认识到区块链巨大的应用价值，但是区块链的技术发展却还没有到达成熟阶段，尤其在企业级应用方面，区块链的***交易并发能力***、***数据存储能力***、***通用性***、***功能完备性***、***易用性***都还存在明显不足。

- ***高并发交易能力***

目前开源的区块链系统的高并发交易能力普遍不高，其中，共识算法是制约性能的重要方面。在区块链中使用的典型共识算法主要有：PoW、PoS、DPoS、PBFT 等，它们的性能对比如下：

Systems		Committee Formation (Resources)	Performances	
			Throughput	Latency
Hybrid	ByzCoin	PoW	1000 tx/s [1]	10–20s [1]
	Algorand	Lottery	90 tx/h [2]	40s [2]
	Hyperledger	Permissioned	110k tx/s [3]	<1s [3]
	RSCoin	Permissioned	2k tx/s [4]	<1s [4]
	Elastico	PoW	16 blocks in 110s [5]	110s for 16 blocks [5]
	Omniledger	PoW/PoX	≈10k tx/s [6]	≈1s [6]
	Chainspace	Flexible	350 tx/s [7]	<1s [7]
proof-of-X	Ouroboros	Lottery	257.6 tx/s [9]	20s
	Snow-white	Stake	100-150 tx/s [9]	–
	Intel PoET	TH12	1000 tx/s [10]	–
proof-of-word	Bitcoin	PoW	7 tx/s	600s
	Bitcoin-NG	PoW	7 tx/s	<1s
	DECOR+HOP	PoW	30 tx/s [8]	60s

表 主流区块链平台的性能对比测试

注：

1 144 nodes/committee.
2 50k nodes/committee.
3 nodes/committee.
4 nodes/committee. 10 committees.
5 100 nodes/committee. 16 committees.
6 72 nodes/committee (12.5% adversary). 25 committees.
7 4 nodes/committee. 15 committees.
8 1 minute average interval; 1 block = 1 MB.
9 40 nodes.
10 As reported in a blog post.
11 proof-of-retrievability. Trusted Hardware.

制约性能的另一个重要因素是账本结构。目前典型的区块链账本设计为区块的单链结构，意味着从全局来看所有的交易都只能顺序地被处理。由于交易处理缺少并行度，因而难以获得接近于传统中心化系统的性能表现。

企业场景下的交易并发量通常要求在每秒处理数百至数千笔以上的交易，远高于目前包括公有链、联盟链在内的典型区块链的表现，而且还要求区块链的性能表现可以随着业务规模的增长而动态伸缩。因此，现实和目标之间存在数量级的差别，需要持续优化和提升区块链系统高并发交易性能。

- ***数据存储能力***

数据存储能力方面，由于区块链的数据只有追加而没有移除，数据只增不减，随着时间推移，区块链系统对数据存储大小的需要也只能持续地增大，在处理企业数据时这一趋势增长更甚。

不同于公链数字货币的主要内容是“账户余额”，企业场景下的数据包含结构化和非结构化数据，数据量十分庞大。以电商供应链为例，主要电商入口的每日的数据记录条数通常都在千万级以上，如再沿着供应链条进一步展开时，每延伸一级数据量都会进一步放大。

目前典型的区块链系统在实现对账本数据的存储时，典型的实现是基于文件系统或者简单的 KV 数据库存储，没有采用分布式存储的设计，因而数据存储能力与实际需要之间也存在较大的差距，需要探索有效的大数据存储方式。

- ***通用性方面***

区块链需要适应多样化的业务需求，满足跨企业的业务链条上的数据共享，这意味着区块链对数据的记录方式要有足够的通用和标准，才能表示各种结构化和非结构化的信息，并能够满足随着业务范围拓展所需的跨链要求。

目前市面上的区块链系统大多采用特定的共识算法，加密算法，账户模型，账本模型，存储类型，缺少可插拔能力，无法适应不同场景要求。

- ***功能完备性***

纵观现有区块链平台，模型抽象单一，难以适应业务系统快速开发的要求。另外，缺少对企业应用中常见的一些功能的支持，例如用户认证、多级授权等。再者，涉及到企业业务协作时，跨企业的事件通知机制显得尤为重要，但少有区块链平台支持。

- ***易用性***

区块链是由多种技术构成，导致学习成本高，实施难度大，人才稀缺。如何让用户快速理解区块链，低成本学习区块链，并将区块链技术快速应到自身的业务中去，目前来看有很大的挑战。区块链技术需要降低学习和使用门槛，支持快速实施部署，提供贴近业务的接口，推广使用。

从比特币的提出到今天为止，人们尝试了非常多样化的应用场景。最初是币（coin）的应用，各种数字货币的出现和热炒引起了广泛关注和讨论。人们发现，作为比特币底层技术的区块链可以用来解决现有业务的一些痛点，创新业务模式。于是金融和产业领域开始形成一些组织联盟，如 R3、Hyperledger 等。技术圈也逐渐将更多的关注从“币”转到了区块链的企业级应用。

人们在许多领域进行了广泛的尝试，例如供应链管理，互联网金融，证券和银行业务，贸易融资，保险，医疗健康，资产管理，数字版权保护，公益慈善，政府公共服务，监管合规性与审计，游戏，公益等等。但是，目前已经成功落地的区块链应用比较少，无论是技术还是业务都还处在摸索阶段。

业界的积极实践进一步巩固和加深了人们对区块链潜在价值的认识，但却鲜有成功的落地案例，大多数停留在理念或 POC 阶段，这种状况的形成受许多因素影响：

- **不适用的、不可持续的场景**

有不少案例是为了区块链而区块链，而不是从解决业务痛点出发，导致案例缺少有效价值，例如对一些不需要公开的信息进行存证。或者没有结合区块链的特点来设计业务创新，仍然以传统的思路来设计业务模式，例如仍然用中心化影响力来把业务简单地搬到链上，不能高效地拓展业务边界。

- **错误的实施方法**

没有充分认识区块链的技术特点，设计出合理的技术方案。比较典型的例子如把区块链简单地当做数据库，把原来中心化系统数据直接搬到区块链上。

- **技术不成熟**

没有充分认识区块链技术目前的成熟度现状，过于乐观地选择技术方案。目前区块链在性能、扩展性、易用性、功能完备性、运维成本等许多方面都还有待完善，更合理的应用方式应该是以应用层业务系统为主，区块链底层完善优化为辅，开展区块链技术应用。

- **人才稀缺**

区块链是个多学科综合技术解决方案，包括分布式、存储、密码学、网络通讯、芯片技术、经济学、法律等，技术专业能力要求高，技术学习、人才培养、实践经验积累周期长。

目前影响区块链应用落地的因素有很多，以上仅简单列举几点，以此说明区块链的发展仍然任重道远。

2. 区块链典型应用场景

区块链有着去中心化、点对点传输、透明、可追踪、不可篡改、数据安全等特点，可以用来解决现有业务的一些痛点，创新业务模式。下面将重点分析和介绍区块链在供应链、金融、政务及公共服务等领域的典型应用场景。这些场景的应用分析基于京东应用区块链技术的经验和京东自身对于区块链技术的应用规划，希望能够通过经验分享引起领域内同行及合作伙伴的共鸣和交流。

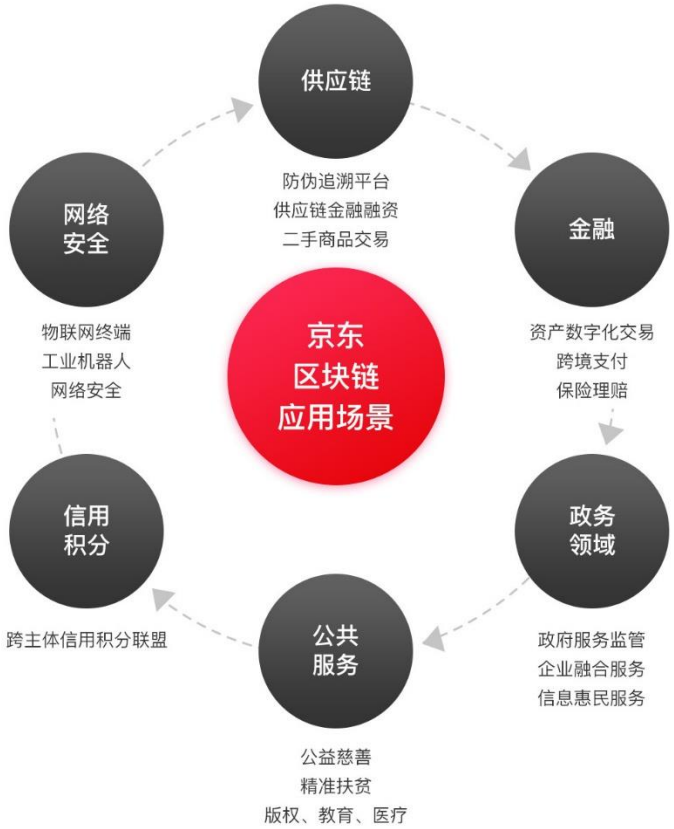

图 京东区块链主要应用场景规划

2.1. 供应链领域

供应链由众多参与主体构成，存在大量交互协作，信息被离散地保存在各自环节各自系统中，缺乏透明度。信息的不流畅导致各参与主体难以准确了解相关事项的实时状况及存在的问

题，影响供应链协同效率。当各主体间出现纠纷时，举证和追责耗时费力。未来企业市场范围越来越大，物流环节表现出多区域、长时间跨度的特征，需要智能高效的防伪追溯能力。

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。

- ***商品防伪追溯***

借助区块链技术，实现品牌商、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。将商品原材料过程、生产过程、流通过程、营销过程的信息进行整合并写入区块链，实现精细到一物一码的全流程正品追溯。

每一条信息都拥有自己特有的区块链 ID“身份证“，且每条信息都附有各主体的数字签名和写入时间戳，供消费者查询和校验。区块链的数据签名和加密技术让全链路信息实现了防篡改、标准统一和高效率交换。

- ***贸易融资***

在供货商、进货商、银行等贸易融资参与主体间建立联盟链，通过区块链记录贸易主体资质、多频次交易信息、商品流转信息等，使贸易双方及银行间公开透明安全地共享真实可信的信息。

针对供应链中的大型企业，银行可以借此丰富融资风控模型，减少线下人工采集和确认信息真实性的工作量，开展动产评估下的融资服务。针对有融资困难的供应链上下游中小企业，可基于区块链提供的主体资质认证、与大型企业的多频次交易信息认证获得信用背书，缓解融资难题。

2.2. 金融领域

金融的核心是信用的建立和传递，区块链以其不可篡改、安全透明、去中心化或多中心化

的特点，天然适用于多种金融场景。

国内外大多数区块链联盟均聚焦于金融领域，例如由 42 家国际银行组成的区块链联盟 R3 致力于利用区块链技术，在解决互信的基础上，构建扁平化的全球一体化清算体系，以提高效率、降低成本。另外，据麦肯锡测算，区块链技术可以将跨国交易的成本从每笔 26 美元降低到 15 美元。高盛也在一份报告中指出，区块链技术将为资本市场每年节约 60 亿美元的成本。

- ***交易清结算***

交易清结算的过程也是交易双方分别记账的过程，在传统的交易模式中，记账过程是交易双方分别进行的，不仅要耗费大量人力物力，而且容易出现对账不一致的情况，影响结算效率。

通过区块链系统，交易双方或多方可以共享一套可信、互认的账本，所有的交易清结算记录全部在链可查，安全透明、不可篡改、可追溯，极大提升对账准确度和效率。通过搭载智能合约，还可以实现自动执行的交易清结算，大大降低对账人员成本和差错率，特别是在跨境支付场景下，效果尤其明显。

- ***资产证券化 ABS***

传统的资产证券化需要结算机构、交易所和证券公司等的多重协调，通过搭载智能合约的联盟链，可以自动实现跨多主体间的证券产品交易。

基于区块链技术的资产证券化管理系统，能够确保消费金融服务公司底层资产数据的真实性，且不可篡改、可追溯，提高机构投资者信心，从而降低消费金融服务公司发行 ABS 的门槛和发行成本，同时还可以进行 ABS 全生命周期管理，及时识别和管控风险。

2.3. 政务及公共服务领域

政务及公共服务的工作核心在于行业标准的制定和有效监督管理，传统管理方式是通过立法和抽查进行监管，不能做到实时监控，涉及仲裁时往往还需要漫长的取证过程。通过搭建包

含政府监管机构、第三方公共服务机构的联盟链，可以探索创新管理机制，实现政务实时监管，并借助区块链的不可篡改、可追溯特性，极大提高仲裁效率。

- ***合同及发票防伪***

电子合同和电子发票的日益普及，为我们日常生活和商业活动带来很多便利的同时，也面临合同造假、发票造假及重复报销等许多新的问题，需要监管部门和企业共同探索有效的解决方案。在开具电子合同、电子发票的同时，通过联盟链完成向监管部门的备案，在发生造假、重复报销等情况时，通过核对已备案电子合同、电子发票的区块链 ID“身份证“，可以快速判定造假事实，确定造假主体，实现实时监管。

- ***公益追溯***

应用区块链技术支撑公益项目的阳光、透明和可追溯。爱心物资经由高效的物流体系直接配送到公益项目地，并由公益机构执行人员发放至受助人手中。捐赠人可通过客户端实时查询所捐赠物资的物流状态，直观地看到物资发放到受助人手中的全过程。

从选购爱心物资开始的全部过程信息、参与主体信息均使用区块链技术防止篡改，确保公益透明性、可追溯，极大增加公益平台的权威性和可信度。

2.4. 其他领域

除了供应链、金融、政务及公共服务领域外，区块链还可以应用在很多其他领域，受篇幅所限，我们不便一一列出，仅举二个例子：

- ***保险防欺诈***

利用区块链共识机制、防篡改机制和可追溯机制，在保险代偿、追偿时提供有效证据支撑，。以车险理赔为例，通常包含车主、4S 店或维修厂、保险公司、交管部门等多个主体，时常发生骗保等理赔欺诈问题。

依托区块链技术和车联网技术，在车辆上安装相应传感记录设备，保证信息的真实、准确

和不可篡改，在出险时，实时或准实时地将车辆事故数据提交给应用区块链技术的“事故认证平台”系统，交警裁决数据、传感记录器数据、维修厂数据等都实时同步，从根本上解决车险理赔欺诈问题，同时提高保险理赔案件的效率和准确性。

- ***大数据安全***

区块链可以解决大数据的安全性问题，保证数据的隐私性。区块链的可追溯特性使得数据从采集、交易、流通，以及计算分析的每一步记录都可以留存在区块链上，使得数据的质量获得前所未有的强信任背书，也保证了数据分析结果的正确性和数据挖掘的效果，能够进一步规范数据的使用，精细化授权范围，追溯数据使用情况，全面保障数据使用的安全合规。

脱敏后的数据交易流通，则有利于突破信息孤岛，建立数据横向流通机制，逐步推动形成基于全球化的数据交易、数据资产保护等全新的应用场景。

3. 京东区块链架构体系

京东区块链的目标是提供企业级的区块链技术与服务，结合自身在大数据、分布式系统方面积累的经验，解决区块链在企业级场景下的交易并发性能、数据存储性能、场景通用性、功能完备性、易用性等方面问题，实现区块链在京东自身的电商和供应链业务的落地，推动京东区块链技术和生态发展。

我们的架构体系由 3 个层次构成：区块链协议、组件框架、平台服务。

图 京东区块链体系架构图

- ***区块链协议***

京东区块链协议作为最顶层的架构设计，定义了区块链的数据格式标准，包括账本状态、历史证明、账本操作集、合约指令集 4 个方面的数据标准。

- ***组件模型***

“组件模型”是区块链逻辑组件的框架模型，是对京东区块链协议的实现框架。包括了共识网络、账本、持久化引擎、合约引擎四个组件。

- ***服务平台***

“服务平台”是对上层的区块链协议和组件模型的具体实现，由网关、服务、节点网络、SDK 和一套工具集组成。

3.1. 设计原则

京东区块链目标是提供企业级的区块链技术与服务，建设具有高性能、良好扩展性、广泛场景通用性、安全合规、接口友好和易部署管理的区块链基础网络设施，打造开放共赢的区块链技术与服务生态。

京东区块链在架构上遵循以下的几个顶层设计原则，确保实现这些具有挑战性的目标。

- **面向业务**

面向业务是京东区块链的第一设计原则。

企业场景的特点是需求非常的多样化，性能要求高。京东区块链定位为企业级的区块链平台，需要适用广泛的企业场景，在设计上首先从定义企业场景的核心用例出发，设计京东区块链的协议、数据结构和功能特性。

- **标准化**

由于区块链应用场景是一种跨主体的有多方参与和协作的场景，京东区块链从顶层开始设计了标准化的协议和数据结构，目标是使区块链真正地成为一种标准化的互联网基础协议。

- **松耦合与模块化**

京东区块链采用模块化设计，通过定义模块间清晰的接口实现模块之间的松耦合，以此获得整个系统的良好扩展性，系统可以根据不同用户和场景的需要，采用不同的可插拔的模块组件。

- **安全可审计**

企业数据的保存需要满足“安全可审计”的要求，京东区块链在设计上将“安全可审计”作为十分关键的一条原则贯穿到每一个功能特性的设计和实现上，设计了可灵活定义的安全访问策略、基于密码学完整地标记数据变化的过程、提供记录级的数据证明。

- **简洁与效率**

京东区块链信奉“大道至简”的架构哲学，可靠和高效的运行来源于简洁的系统设计。京东区块链在协议设计、组件模型、系统实现、外部接口、部署管理各个方面都认真地遵循这一原则。

3.2. 设计方法

区块链是一种全新的架构形式：a、从技术视角看，区块链是一种健壮和安全的分布式状态机；b、从业务视角看，区块链是一种面向业务的跨多主体的数据协议。

区块链将成为一种新形式的互联网协议，它能够使跨主体的业务协作变得简单、高效和安全。与传统的互联网协议不同（如 TCP/IP，HTTP 等），传统协议都是面向通讯过程的，而***区块链是面向业务过程的。***

如果以应用开发者的视角来观察一下基于区块链的应用开发过程，会更清楚地察觉这种巨大的差异。

假设要开发一个商品贸易系统，业务的参与者包括贸易买卖双方和物流企业，这个系统要帮助买卖双方建立交易合同、跟踪货物运输过程、交付结算。基于区块链实现该应用通常需要以下几个步骤：

（1） 定义参与业务的各个主体的身份账户

为参与者注册登记一个由公私钥对（证书）表示的身份账户。由符合国家标准的证书所表示的身份账户是能够代表一个特定的法人，由该账户签发的数据可以在法律上被认为是该

法人做出的确认。

传统的架构方案通常是 SOA：各个参与方的系统发布各自的 SOA 接口，相互间通过 SOA 接口调用实现系统对接。在这种架构下，开发者实现任何一个特定参与方的业务角色的功能，都需要把该参与方的身份与其公布的 SOA 服务接口的通讯地址建立对应关系，开发者对业务功能的实现是体现为对通讯接口的调用和处理。然而，这种方式调用获得的数据难以具备防篡改能力的（尤其是大量数据量情况下），也难具有对方法人签名确权的效力（若对每条数据记录都进行签名则技术实现成本很高）。

（2） 编写智能合约对业务过程做出定义

把参与者之间达成的商业协议以智能合约代码的形式进行定义，以数字化形式约定贸易的商品属性、数量、交付价格、交付期限、交付条件、运输方式、交割检验标准、货款计算方式、货款支付时限等等。

在智能合约的编写过程中，需要关注的内容通常有：在账本中保存的业务信息的格式；业务过程中产生的业务状态；改变业务状态需要满足的条件；业务状态变更的触发方式；业务状态变更涉及更新的业务信息。

智能合约代码的编写过程是完全不需要关注非业务功能的处理，比如：业务数据在参与者之间网络结构、寻址方式、通讯协议、传输格式、响应线程、处理资源。

智能合约虽然也表现为某种形式的编程语言，但是其编写逻辑是完全直接面向业务的，可以形式化地概括为 3 个方面：

a、定义多主体间的业务数据格式；

b、定义业务过程包含的业务状态表；

c、定义各个业务状态的转换条件和触发方式。

（3） 联合签署智能合约并触发业务初始条件

智能合约最后需要经过参与者以各自的身份账户做出签署，之后每一方参与者只需要根据自己业务范围内的业务进程做出相应的操作，便触发了智能合约的执行。

在这个过程中，区块链系统以客观的技术手段提供以下几个方面的保证：

- 确保合约在每一个参与业务的主体的节点上被一致的执行，并得到一致的结果；
- 确保合约执行过程的每一个步骤都被准确地记录下来；
- 确保合约执行过程的记录以及最终结果都无法被篡改；
- 确保参与的主体对合约执行过程的记录以及结果进行签名，确保合约被执行的事实在今后都不可抵赖。

从这个抽象的例子中可以看出，区块链是一种全新的面向业务的架构体系。

3.3. 账本协议

账本协议是从数据的角度定义的一个标准模型，包含两个方面的定义：

- **账本数据的标准格式**

由两部分构成：

a) “账本状态”表示当前实时的数据内容；

b) “历史证明”表示账本数据的特征以及数据变更历史的特征。

- **读写账本数据的指令的标准格式**

由两部分构成：

a) “账本操作集”定义了对账本数据的写入操作类型的标准表述以及参数的标准格式。

b) “合约指令集”定义了标准化的合约语言指令格式。

定义账本协议的目的是让链上的数据可以被标准化地进行交换、验证、存储和使用，能够跨越不同技术实现的区块链网络，无关特定的数据存储实现。

3.3.1. 账本状态

“状态”一词在此是一个计算机领域的概念，在此表示区块链系统在某一时刻所处的状况，由系统保存的业务数据以及系统运行的控制属性构成。

京东区块链的 “账本状态”由“身份”、“KV 数据”、“权限”、“合约代码”组成。

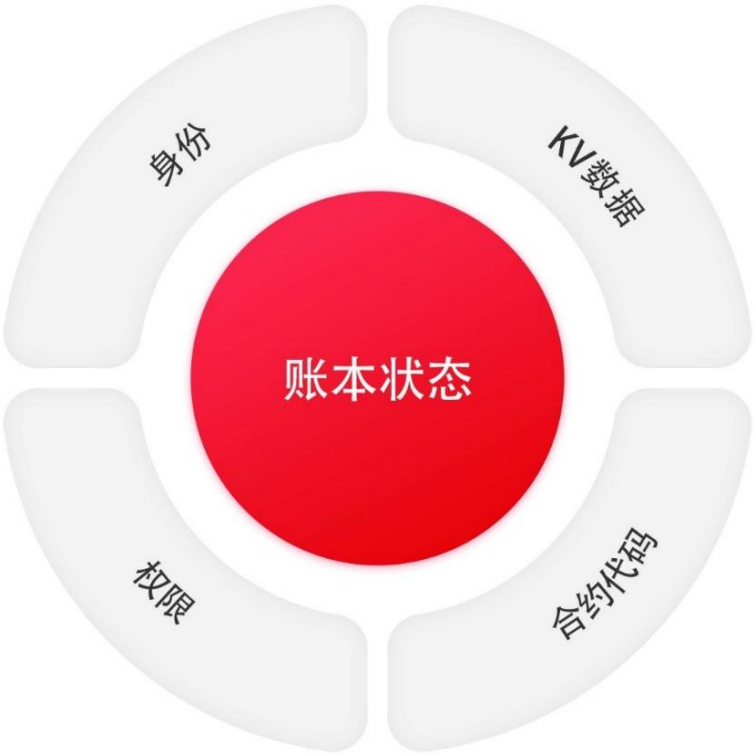

图 京东区块链账本状态示意

- “身份”由一个“区块链地址（Address）”和相应的非对称密钥对/证书表示；
- “KV 数据”是账本数据表示形式，通过键（Key）唯一标识，通过值（Value）记录内容；
- “合约代码”表示状态变更的逻辑，以合约指令序列表示；

- “权限”是“身份”对“KV 数据”和“合约代码”的访问控制码

3.3.2. 账本操作集

“账本操作集”是为了实现跨链互操作而定义一个通用的标准，包含“类型”的标准码，“参数”的标准格式。

典型的操作包括：

- 身份注册
- 状态数据读写
- 合约部署
- 合约调用
- 权限设置

3.3.3. 合约指令集

区块链以合约语言的形式定义业务状态的控制和转换逻辑。

通过设计一个标准化的合约语言指令集，可以用一种通用的方式来表述各种复杂的业务逻辑，从而与具体的编程语言无关。

一方面，遵循标准的合约指令集，区块链系统能具备良好的通用性；

另一方面，开发者可以用不同编程语言编写智能合约，降低了学习使用门槛，满足不同企业的团队技术栈要求。

3.4. 组件模型

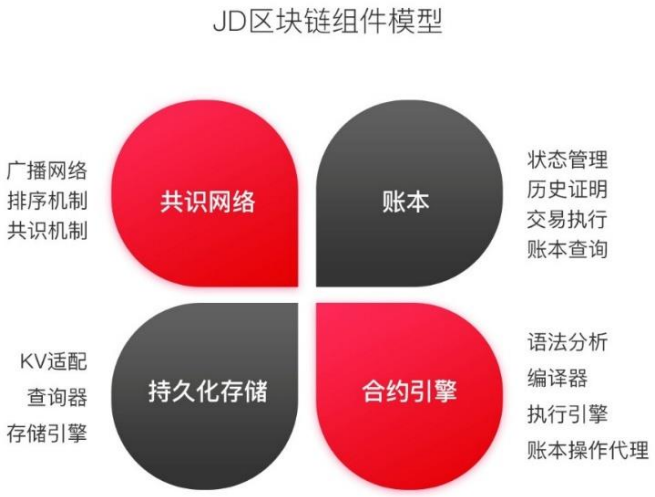

图 京东区块链组件模型

“组件模型”是一个逻辑上的功能模块设计，是实现账本协议的逻辑框架。定义了组件的标准化接口，使得遵循组件模型的区块链系统实现具备松耦合、可插拔的特性。

3.4.1. 共识网络

目前典型的共识算法主要有 PoW、PoS、PBFT、Raft、Paxos 等。通过对比发现，这些算法在运行过程都可以抽象下面几个阶段：

（1）交易扩散；

（2）交易排序；

（3）调用交易执行程序；

（4）对交易执行结果进行共识；

（5）提交共识结果。

各种共识算法的差异体现在不同阶段采取了不同实现策略。

- PoW、PoS 算法在交易扩散和排序时，不采用原子广播协议，同时以随机化的方式选择出 leader 节点执行排序，因此会导致交易可能被随机丢弃。

- Raft、Paxos 算法对全部交易进行原子广播和排序，但在共识的过程并不处理拜占庭错误。
- PBFT 算法对全部交易进行原子广播和排序，同时在共识阶段处理拜占庭错误，不支持动态调整节点。

我们从面向企业级应用场景的特点出发，选择类 BFT 的算法进行优化，提供了确定性交易执行、拜占庭容错、动态调整节点的特性。

京东区块链的共识网络组件按照模块化的思路设计，基于以上几个通用阶段进行封装，抽象出可扩展的标准接口。

3.4.2. 账本

账本状态与合约分离，使用基于身份的访问控制协议约束合约对状态的访问，这种将数据与逻辑分离的设计模式是典型的贫血模型，可为上层业务逻辑提供无状态的逻辑抽象。

3.4.3. 持久化存储

将账本信息的持久化格式定义为更简洁的 KV 格式数据，使得可以利用成熟的 NoSQL 数据库来实现持久化存储。基于目前在 NoSQL 数据库上成熟的海量数据存储方案，使得区块链系统能支持海量的交易。

3.4.4. 合约引擎

合约引擎包含两大部分，前端包括合约高级语言规范及其工具链，后端是一个轻量级的合约中间代码的执行环境。所有对账本的操作通过账本组件提供的 API 实现。

3.5. 服务平台

功能模块分为区块链网关、区块链节点服务、区块链基础网络、配套工具四个部分。

图 京东区块链服务平台

3.5.1. 区块链网关

“区块链网关”被设计为一种轻量的网关系统，通常是部署在参与者的网络环境中，提供功能包括：

a) 私钥管理：提供完全本地化的私钥保管功能；

b) 隐私保护：采用端到端加密手段实现隐私保护；

c) 协议转换：提供轻量化的 HTTP Restful Service ，适配 TCP 协议的区块链节点 API。

3.5.2. 区块链节点服务

在区块链基础网络的基础上提供的面向应用的通用的功能组件，目的是提供通用功能的复用，包括：

a) 面向应用的账户管理；

b) 账户的认证授权；

c) 面向对象的账本数据访问框架；

d) 事件通知机制；

e) 智能合约管理。

3.5.3. 区块链共识网络

由共识节点组成的网络，基于 P2P 网络和共识算法确保交易数据在节点之间保持一致。

3.5.4. 工具

配套的工具集合，包含 SDK、数据管理、安装部署工具、监控服务。

3.5.5. 部署架构

京东区块链支持以下几种部署模式：

a、 参与主体维护完整的共识节点，好处是参与者可持有数据，但需要付出运维成本；

b、 参与主体仅维护网关节点，通过公共的共识节点接入区块链，好处是便于自行管理私钥，且维护成本低，但网关节点不持有数据；

c、 参与主体通过公共的网关节点接入，适用于 2C 场景，用户可以基于公共的网关节点托管私钥；

d、 监管方可以只部署“备份节点”，从其它节点同步数据作为备案；

e、 监管方还可以部署共识和网关节点，对公众开放查询，作为“存证公示”。

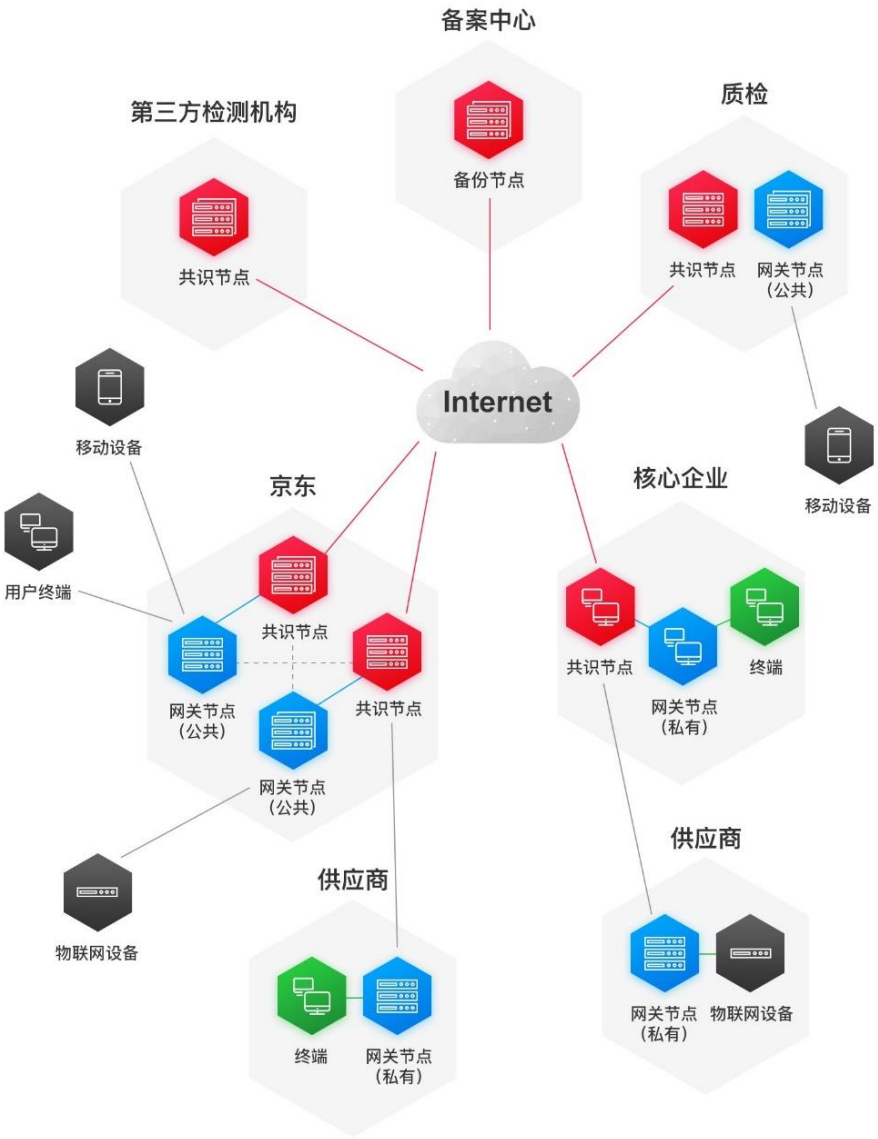

图 京东区块链的部署架构

4. 京东区块链的特点

京东区块链项目的目标是建立一种适用于广泛应用场景、满足企业应用需求、开放和易用的区块链技术体系和系统服务平台。在京东区块链研发和应用的过程中，我们始终关注性能、功能、安全、合约、合规五个方面，并在这五个方面着重开展区块链技术能力的优化。

4.1. 性能

- 采用优化的 BFT 共识协议和 P2P 通讯，支持多链并行共识；
- 采用面向消息的高并发处理架构，支持横向伸缩，并行处理海量交易。
- 支持横向伸缩存储和在线动态扩容，以实现海量数据；
- 采用灵活的数据存储结构，支持冷热数据分离；
- 支持节点动态加入和退出，实现系统的高可用性，保证业务不间断运行。

4.2. 功能

- 支持用户实名与认证；
- 支持企业数据治理;
- 支持事件驱动的业务协作模型;
- 支持多账本以实现按业务维度管理链上数据。

4.3. 安全

- 可插拔的密码算法，可以灵活的制定相应的密码体系；
- 平台默认实现多套密码算法，包括国密算法和硬件加密设备。

4.4. 合约

- 支持可复用的智能合约；
- 支持智能合约语言的调试功能。

4.5. 合规

- 支持基于 CA 的账户认证；
- 支持监管节点的接入；
- 支持数据备案。

5. 共创信任经济时代

信任经济，京东的定义是“低欺诈、高可信的商业经济环境，保障参与交易的主体低成本、低风险的完成交易，信息全程可追，问题可查”。信任经济实现的基础是交易信息的全面数字化，具备较强的数据可信保障机制和验证机制。

区块链的本质是通过一系列的技术整合，建立一套公正、透明、可信的规则，结合物联网对现实世界数据的采集，以及人工智能算法搭建的自动交易和激励系统，在未来有望建立一套无人值守的价值数据交换和交易体系，将人类社会带向数字化的信任经济时代。

京东商城是以自营零售发展壮大的新一代零售企业，在我们的生态体系中有大量的政府指导部门，品牌商、物流服务商、学术研究机构、咨询机构等合作伙伴。每个时刻在京东的无界零售网络中，都在产生着海量的大数据，这些数据需要在不同主体间进行整合、流动、交易，甚至是作为企业数据挖掘的生产资料。提升数据的公信力与可信度，降低数据校验和交易的成本，提升整个社会价值链的运转效率，是数字化经济下，每一个企业主体面临的挑战和必须承担的社会责任。京东愿意积极配合政府主管部门，建立国家区块链技术标准和规范，探索更多的区块链应用场景，推广区块链技术，共同创建基于区块链的信任经济生态。

如果说区块链是构建合作伙伴间信任经济的基石，那么就需要区块链或是联盟链在互联网的广泛部署和规模化应用，但正如前面白皮书章节中的介绍，目前区块链技术推广仍存在诸多挑战，京东区块链技术团队总结和建议如下：

（1） 政策与标准指导

区块链规模化应用，需要在跨企业达成一致的技术标准和行业监管标准，在这方面京东和各企业都积极拥护国家各级政府部门的政策指导，近期留意到工信部正牵头筹建区块链技术标准委员会，期待国家区块链技术标准尽快落地，供各企业参考。在政策和标准方便，京东建议国内领衔的科技与互联网公司积极组建区块链技术联盟，互通

有无，共同推进技术的应用、分享和标准落地；

（2） 技术平台的不断完善

区块链技术脱胎于比特币公共网络，据不完全统计，比特币矿池每年消耗大量的电力资源，原因是完全公有链的区块链部署形式实际上并不适用于全部场景。京东在实际应用区块链技术的过程中，留意到读写性能、联盟链动态组建、垂直应用 API 插拔化支持、快速部署等一系列亟待解决的技术难题，需要对区块链技术应用支持的各方一同参与、交流和共同解决；

（3） 在应用中建立激励机制和商业模型

比特币作为区块链的创始级应用得益于它搭建了一套非常完善的公有链模型和基于这个模型的工作和激励机制。以供应链的防伪追溯场景为例，京东投入巨大的研发资源落地并面向社会免费开放了 SaaS 化的区块链防伪追溯平台，但在推动各品牌商接入平台时，却发现品牌商对于数据上链追溯的动力不足。如何通过商业模式建立较好的区块链应用场景的激励机制，让各区块链应用真正产生商业价值，是区块链规模化应用的核心挑战之一。

一项伟大的技术从萌芽到规模化应用，都需要经过一个漫长艰辛的过程，在这个过程中创新精神、协同意识是取得阶段性胜利的必要条件。区块链技术本身就是一项“去中心化”的技术，因此在其应用的过程中，必然需要各方伙伴的协同共进，大家携手推动各自区块链平台的桥接，建立技术共享和问题磋商机制，在区块链技术广泛改造互联网基础设施的明天，坚信我们必将迎来信任经济的新时代！

6. 术语解释

1、交易

在本文中是一个计算机术语，英文表述为 Transaction，等同于另一个计算机术语“事务”的含义，并非指商业语境中的交易，只因在区块链的语境中已经约定俗成地翻译为“交易”，本文遵循了这一习惯。

2、虚拟机

在本文中是指状态机技术，而非一般所说的虚拟化技术（如：VMWare）,是智能合约的编程语言的运行环境。

3、分布式

分布式系统是由一组通过网络进行通信、为了完成共同的任务而协调工作的计算机节点组成的系统。

4、共识机制

共识是分布式系统中的一个过程，用于在涉及多个不可靠节点的网络中，在所有节点之间实现数据一致性并对某个提案达成一致。

5、UTXO

Unspent Transaction Outputs 的英文缩写，即未花费的交易输出，是一种数字货币区块链经常采用的一种账户模型设计。在此模型中，每一笔交易都应该有 N 个交易输入，同时产生 M 个交易输出（N 与 M 可以不等）。其中交易输入是前序任意交易的未花费的交易输出，如果当前交易成交，该前序交易的输出也就变成了成交的交易输出，也就失去了成为交易输入的资格。UTXO 模型能够追踪数字货币的流向：未花费的交易输入告知货币是从哪里来的，未花费的交易输出告知货币往哪里去。

6、PoW

Proof Of Work 工作量证明共识算法，在比特币中被首次提出。数字货币矿工们通过随机哈希计算获得当前区块的记账权，从而获得区块奖励。PoW 的特点是哈希计算随机，难以弄虚作假，且容易被验

证。但另一方面，矿工们间的哈希计算竞争浪费了大量资源。

7、PoS & DPoS

Proof Of Stake 权益证明共识算法，PoW 的替代方案。根据节点所占权益比重，决定其获得区块记账权的概率，权益越多，越有机会获得区块记账权。DPoS 在 PoS 的基础上更近一步，节点将权益委托给其他节点，由其代表自己行使权力。

8、Paxos

Leslie Lamport 于 1990 年提出的一种基于消息传递且具有高度容错特性的一致性算法，它解决的问题是在一个可能发生上硬件故障、网络延迟、消息丢失等异常的分布式系统中各参与者如何就某一值（提案）达成一致。9、PBFT

9、PBFT

实用拜占庭容错算法，是 Miguel Castro (卡斯特罗)和 Barbara Liskov（利斯科夫）在 1999 年提出来的，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。

10、 智能合约

智能合约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。智能合约概念于 1994 年由 Nick Szabo 首次提出。智能合约的目的是提供优于传统合同方法的安全性，并减少与合同相关的其他交易成本。

参考文献

（1）麦肯锡：《区块链-银行业游戏规则的颠覆者（2016）》

（2）Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. (2008)

（3）Maziéres, D.: The Stellar consensus protocol: A federated model for internetlevelconsensus, November 2015.

（4）Brown, R. G. (2016). Introducing R3 Corda: A Distributed Ledger for Financial Services.

（5）工信部：《中国区块链技术和应用发展白皮书（2016）》

（6）UK Government Chief Scientific Adviser: Distributed Ledger Technology: beyond block chain

（7）Goldman Sachs：Blockchain-Putting Theory into Practice

（8）Buterin, V.: A next generation smart contract and decentralized application platform

（9）Zindros D.: Trust in decentralized anonymous marketplaces.

（10） Swan M.: Blockchain: Blueprint for a new economy.

（11）Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts.

（12）G Zyskind, O Nathan: Decentralizing privacy: Using blockchain to protect personal data.

（13）Schwartz D, Youngs N, Britto A.: The Ripple protocol consensus algorithm.

（14）Bonneau J, Clark J, Goldfeder S.: On Bitcoin as a public randomness source.

（15）Kiayias A, Panagiotakos G.: On Trees, Chains and Fast Transactions in the Blockchain.

（16）Miller A, LaViola JJ Jr.: Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin.

（17） Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, Pieter Wuille: Enabling blockchain innovations with pegged sidechains.

（18） Lewenberg Y, Sompolinsky Y, Zohar A.: Inclusive Block Chain Protocols.

（19） Bentov I, Mizrahi A, Rosenfeld M.: Decentralized Prediction Market without Arbiter.

（20） J Yli-Huumo, D Ko, S Choi, S Park, K Smolander: Where is current research on blockchain technology?—a systematic review.

（21） Babaioff M, Dobzinski S, Oren S, Zohar A.: On Bitcoin and Red Balloons.

（22） M Pilkington: Blockchain technology: principles and applications.

（23） J Mattila: The Blockchain Phenomenon–The Disruptive Potential of Distributed Consensus Architectures.

（24） Benet J.: IPFS - Content Addressed, Versioned, P2P File System.

（25） GW Peters, E Panayi: Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money.

（26） Nick Szabo: Smart Contracts: Building Blocks for Digital Markets

（27） Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi , Patrick McCorry , Sarah Meiklejohn , and George Danezis: SoK: Consensus in the Age of Blockchains

京东

咨询与合作 Y@jd.com