# 中国区块链产业发展报告

# (2018-07)

# 一、 总体现状

## 1.1 企业数量及投资

截至 2018 年 3 月底，我国以区块链业务为主营业务的区块链公司数量达到 456 家，单季度增长 22 家。企业数量自 2016 年起进入显著增长期，2016 及 2017 年均超过 100 家。

与新增企业数量相呼应，从 2016 年开始，区块链领域的投资事件达到 60 起，是 2015 年的 5 倍，在 2017 年进一步增加达到接近 100 起。在今年第一季度，区块链领域的投资事件数量就达到了 68 起，超过 16 年全年，预计将会创历史新高。

融资轮次方面，目前有接近 90%的投资事件集中在早期阶段（A 轮及以前），B 轮及以后的投资事件占比仅为 2%，另外有 9%的投资事件属于战略投资。由此可见，区块链产业在中国目前还处于相当早期的阶段。随着整个产业的发展以及项目落地速度的加快，融资轮次将逐渐往后延伸。

## 1.2 产业链及投资

目前我国区块链产业链条已经基本形成，从上游的硬件制造、平台服务、安全服务，到下游的产业技术应用服务，到为产业配套的行业投融资、媒体、人才服务，各领域的公司已经基本完备。

从区块链产业细分领域新成立公司分布状况来看，截至 2018 年 3 月底，区块链领域的行业应用类公司数量最多。第二梯队为底层平台、解决方案和媒体社区类公司，在 40 家以上。

与新增企业所属领域相呼应，行业应用服务相关的公司获投事件数最多，总共达到了 113 起，可见投资人对于有具体的应用场景，能够实际落地的项目越来越看重。

## 1.3 应用方向

区块链的各类特性提供信任机制，具备改变金融基础架构的潜力（去中介化）。金融方面，目前已在支付清算、信贷融资、证券、保险、租赁等细分领域落地应用。例：微众银行通过基于区块链的机构间对账平台把对账时间从 T+1 日缩短至 T+0，实现了日准实时对账。（大型场景的应用，崭新的金融业务模式）

实业方面，随着区块链技术创新发展逐步成熟，产业应用的实际效果愈发显现，区块链的应用已从金融领域延伸到实体领域，电子信息存证、版权管理和交易、产品溯源、数字资产交易、物联网、智能制造、供应链管理等领域。例：沃尔玛食品供应溯源。

从应用范围看，区块链技术几乎在所有的产业场景都能落地应用，原因是几乎所有的产业场景都涉及交易，都有降成本、提效率、优化产业诚信环境的需求。在企业内部，信息化水平往往已经比较高，各类管理系统已经非常先进，但是在企业之间协作的环节，很多情况下并没有被

信息系统所覆盖。因此，很多联盟链系统都实际上是在解决这个问题，在“弱信任”环境中让多种业务主体平等交流，信息共享。

# 二、 竞争格局

## 2.1 互联网巨头布局

BATJ 纷纷加入区块链技术的研究与场景应用。

百度：百度金融先后与华能信托、 长安新生等落地了国内首单区块链技术支持证券化项目和区块链技术支持交易所 ABS 项目。

阿里巴巴：公益、溯源、互助保险等，申请专利数量已达到 80 件左右

腾讯：基于 Trust SQL 核心技术，打造领先的企业级区块链基础服务平台。目前，腾讯区块链已经落地供应链金融、医疗、数字资产、物流信息、法务存证、公益寻人等多个场景。例如，腾讯基于供应链场景下的真实交易数据， 通过腾讯区块链技术及运营资源帮助小微企业融资。

京东：运用区块链技术搭建“京东区块链防伪追溯平台”，让所有生产、物流、销售和售后信息分享进来，共同铸建完整 且流畅的信息流；ABS。

## 2.2 地域分布

北京、上海、广东、浙江合计占比超 80%。其中，北京以 175 家公司、占比 38%处于绝对的领先地位。第二梯队有江苏、四川等省份。活跃度最高的城市为北京、上海、深圳、杭州。随着未来区块链项目与传统产业场景结合度的提高，区块链项目在国内的地域分布将进一步扩展。

## 2.3 国际竞争

目前，区块链逐渐成为“价值互联网”（自带金融属性的互联网络，资产可以像信息一样流动，该网络中第三方中介系统不再是必需的)的重要基础设施，很多国家都开始积极拥抱区块链技术，抢占新一轮产业创新的制高点。截至 2017 年末，全球区块链创业公司超过 1600 家，获得融资的公司分布在全球 45 个国家和地区间，融资总额近 20 亿美元（投中研究院）。全球 9 成的政府正在规划区块链投资，并将在 2018 年进入实质性阶段。

专利方面，美国公开专利数量从 2014 年的 150 件增加到 2017 年前 7 个月的 390 件，中国公开专利数量从 2014 年的 2 件增加到 2017 年前 7 个月的 428 件，中国区块链专利公开数量增速超过美国。

私募融资规模方面，2014 至 2016 年期间，虽然中国私募股权融资规模小于美国，但增长速度明显高于美国。

美国：企业数量与融资额仍领跑全球。将区块链上升到“变革性技术”，成立国会区块链决策委员会
欧盟：分布密集。

# 三、 政策及监管环境

## 3.1 政策支持

区块链技术已经上升到国家科技战略层面。2016 年 12 月，《国务院关于印发“十三五”国家信息化规划的通知》中首次提及区块链，并将其与量子通信、人工智能、虚拟现实、大数据认知分析、无人驾驶交通工具等技术一起作为重点前沿技术，明确提出需加强区块链等新技术的创新、试验和应用，以实现抢占新一代信息技术主导权。
其次，相关行业、国家和国际标准也在加速制定，解决区块链的关键技术标准问题。为把握区块链产业发展机遇，抢占区块链产业发展制高点，各地政府及时出台区块链技术和产业发展扶持政策：贵州（2016），广州/南京/山东（2017），河北（2018）。

## 3.2 监管环境

区块链备案平台及如金丘科技、众享比特等监管科技公司在促进区块链监管体系的形成。

# 四、 本产业细分领域现状

## 4.1 底层平台

平台领域是整个产业中的热点，创业公司和大公司纷纷在布局区块链底层平台。目前的三种主流平台模式为公有链、联盟链及 BaaS。

### 4.1.1 公有链

公有链最符合区块链的本质，被看作是未来区块链领域最有前景的方向。公有链的优点包括：能够保护用户免受开发者的影响；所有交易数据都默认公开；能够通过社区激励机制更好地实现大规模的协作共享等。
另一方面，基于底层公链的区块链应用也将迎来大爆发，DAPP 时代即将来临。DAPP 之于底层公链，就如同 APP 之于 IOS 和 Android 系统，未来可能会衍生出一个新的生态体系。
对于公有链来说，节点数越多意味着系统的安全性和公平性越高，但同时意味着系统效率的低下，因为每增加一个节点，就需要多达成一次共识。例如：比特币每秒能处理 7 笔交易，以太坊每秒能处理 20-30 笔交易。由于 TPS 太低，导致比特币和以太坊等公链普遍存在交易费用高、确认时间长等问题。

目前在公有链领域，我国技术处于世界先进水平，已经诞生了几家比较领先的底层平台公司如小蚁（NEO）。

#### 4.1.2 联盟链

联盟链被认为是“部分去中心”或者“多中心”的区块链，链上数据只允许系统内的成员节点进行读写和发送。

联盟链让节点数得到了精简, 在单位时间内能够确认的交易数量要比公链大很多，更容易在现实场景中落地。此外，联盟链相对于公有链非常重要的特点就是节点准入控制与国家安全标准支持，可通过制定准入和监管规则符合监管要求。

国外典型案例：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，吸引了包括华为、腾讯云、百度金融、三星、IBM、英特尔、Cisco、Oracle 等众多公司参与，目前已经有超过 200 家会员单位。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。

国内典型案例：微众银行自 2015 年开始投入资源探索区块链技术，目前已研发了两大区块链开源底层平台。其一是联合万向区块链与矩阵元共同推出企业级联盟链底层平台 BCOS，并在 2017 年 7 月完全开源。随后，又联合金链盟开源工作组的多家机构共同研发并开源了 BCOS 的金融分支版本——FISCO BCOS，目前已有数十家企业基于 FISCO BCOS 平台，聚焦区块链应用场景的落地，在包括供应链、票据、数据共享、资产证券化、征信、场外股权市场等场景进行实践。

#### 4.1.3 BaaS

BaaS（Blockchain as a Service）通常是一个基于云服务的企业级的区块链开放平台，可一键式快速部署接入、拥有去中心化信任机制、支持私有链、联盟链或多链，拥有私有化部署与丰富的运维管理等特色能力。

目前，大公司在 BaaS 方面的动作更加活跃，因为它们都有自己的云服务，并且生态体系内的业务场景丰富，适合根据具体的业务场景来试错和反推平台服务。此外，由于公有链的共识机制导致系统效率低下，而 BaaS 是基于对大公司的平台信任，去构建部分去中心化或者弱中心化的架构，从而在一定程度上达到可信化和效率的兼顾。

腾讯区块链 BaaS 开放平台，定位于打造领先的企业级区块链基础服务平台，专注于帮助企业快速搭建上层区块链应用场景。目前，腾讯区块链 BaaS 开放平台提供共享账本和数字资产两大业务模型。共享账本模型主要适用于解决信息不对称、提供存证证明等需要进行信息有效性共享的场景。数字资产模型主要针对可数字化的资产交易场景，能够有效防止数据篡改,规避数据伪造风险。

### 4.2 数字资产储存（数字钱包）

区块链产业的发展需要有新型的数字资产存储方式，这就催生了数字钱包的诞生。对于数字钱包来说，安全性需求永远是排在第一位的。近几年，数字资产安全问题屡见不鲜，数字钱包作为区块链产业链上一个重要环节，需要打造更加安全可靠的存储环境。

数字钱包的主要作用是帮助用户管理和使用私钥——数字加密资产所有权的唯一凭证。目前，数字钱包类型主要分为冷钱包（不联网，不怕黑客窃取私钥）和热钱包等。IT 桔子的数据显示，截至 2018 年 3 月底，中国开发数字钱包的相关公司数量大约有 15 家，基本上都是以开发热钱包为主。

去中心化钱包的特点包括：第一、私钥是用户自持，当然密码也是用户自持；第二、资产是存储在区块链上，而不是托管在中心化的服务器上，并且目前也无需实名认证，即可生成钱包；第三、无法实现“账户冻结”、“交易回滚”等操作。因此，用户也不用担心钱包服务商出现监守自盗的情况。

例如： 猎豹移动在海外推出移动安全数字资产安全钱包 SafeWallet，该钱包引入了三层安全防御体系（用户行为安全、手机防御安全、资产安全管理）。

## 4.3 解决方案

区块链解决方案主要是指在底层平台的基础上进行扩展，目的是便于开发者基于区块链技术开发出产品和应用，或者是服务商直接为客户提供针对具体业务场景的解决方案。

ChainSQL: 众享比特推出的基于区块链的数据库应用平台，将区块链技术与传统数据库技术结合，打造不可篡改、安全、一致、低成本的数据库。

## 4.4 硬件制造和基础设施

区块链硬件制造和基础设施起源于区块链的共识机制之一——POW（Proof of Work，工作量证明机制），即全网计算节点通过算力竞争记账权，来获取经济奖励。

发展路径：个人计算机到专业矿机，专业矿机中 FPGA（可编程门阵列）过渡到 ASIC（专用集成电路）

在区块链硬件领域，中国的相关公司具有绝对优势，全球大部分区块链硬件均由中国厂商生产。世界排名前三的区块链硬件设备厂商比特大陆、嘉楠耘智和亿邦科技，均是中国公司的。在算力的军备竞赛下，谁的区块链硬件算力更强，就能抢占更多的市场份额。芯片的设计和研发能力，是这场军备竞赛的决定性因素，因此，非常有力地促进了我国专用芯片设计产业的创新发展。

嘉楠耘智的主营业务是专用集成电路（ASIC）芯片以及衍生设备的研发、设计及销售，并提供相应的系统解决方案和技术服务。截至 2017 年 12 月底，嘉楠耘智累计售出基于 28nm 以及 16nm 技术芯片设备总算力约为 2000P，占同期公有区块链全网新增算力的 25%以上，并且是台积电（全球最大晶圆代工厂）中国北方区最大客户。此外，嘉楠耘智发布了全球第一款量产人工智能芯片 KPU。

## 4.5 安全服务

针对目前区块链存在的底层代码、密码算法、共识机制、智能合约、数字钱包等安全问题，该领域也出现了一些提供安全服务的公司，它们主要通过技术手段、代码审计帮助客户解决各种区块链安全问题。

例如，成都链安科技有限公司，开发了面向区块链智能合约安全性和功能正确性验证平台 VaaS。目前，VaaS 平台已支持主流区块链平台（如以太坊、EOS 等）。

再如，厦门慢雾科技有限公司，专注区块链生态安全，已经为全球多家知名区块链公司做了安全审计与防御部署，作为第三方审计单位审计了 200 多份以太坊智能合约，累计发现数十个高危、中危安全问题。“慢雾区”区块链安全社群已累计辐射人数达 10 多万人，社区内不乏区块链的从业人员。

## 4.6 媒体及社区

IT 桔子的数据显示，截至 2018 年 3 月 31 日，区块链媒体及社区领域的新公司数量为 58 家，投资事件数量为 28 起，融资额多在数百万、千万乃至上亿级别。其中，仅 2018 年第一季度该领域就发生了 18 起投资事件，包括：火星财经、巴比特等均拿到了投资。区块链媒体及社区也成为当季区块链产业的一个热门投资方向。

对于一个新赛道而言，如果先投资一家行业媒体，可以用来了解整个行业的信息，以及掌握一定的舆论权，这也是很多投资人会选择从投资媒体来入局区块链领域的原因。

目前，区块链媒体及社区领域的创业，主要还是以行业新闻、快讯、深度报道、行情、数据、社区、社群等形式为主，与其他的媒体形式并没有本质差异。从商业模式来看，该领域的公司基本上还是以广告收入为主，另外会衍生出一些相关的培训、活动会务、评级、数据等增值服务，盈利模式也没有超出传统范畴。现在很多区块链媒体的同质化严重，对于众多的区块链媒体入局者来说，洗牌期即将到来。

## 4.7 行业组织和行业研究机构

从 2015 年 12 月到 2017 年底，在国内成立的与区块链相关的联盟/协会已经达到了近 20 个。这些组织为行业内人士提供了一个专业的交流与合作平台，对于促进中国区块链产业健康发展和加快应用落地起到了推动作用。

此外，由于区块链产业的高速发展，导致了人才短缺问题严重。因此，全国各地区的相关高校已经开始开设相关课程。例如：清华大学 iCenter、浙江大学软件学院、同济大学金融科技研究院。

# 五、 发展趋势

## 5.1 政策导向

在下一轮国际竞争中，公链等区块链底层架构和基础设施具有较高的重要性，特别是服务于民生领域、公共安全等领域的区块链基础设施，对于保障社会食品药品安全、加快构建社会信用体系、增加人民群众的获得感有重要意义。因此，有必要由国家统一监管，建立一套公开透明、可溯源、信用可有效传递的基础设施。

## 5.2 从金融到实业

当前，区块链技术落地的场景已从金融领域向实体经济领域延伸。未来三年将是传统行业与区块链更紧密融合的时期，随着区块链开始改变市场结构，企业将会关注到商业的变革，带有智能合约技术的新生态系统会被整合到在现有行业中，新型的商业模式和监管服务模式将会涌现，社会企业数量将会大大增加。跨链技术将实现不同区块链之间，甚至区块链和传统 IT 系统之间的价值流转。结合区块链技术目前的发展速度和现有技术、市场、监管体系的成熟程度，可以预见区块链生态在三年之内将实现广泛落地，与具体产业场景深度相结合，创造出新模式，切实推动实体经济转型升级、提质增效。

目前，实体经济成本高、利润薄，中小微企业融资难、融资贵、融资慢等现象仍然存在，金融对实体经济支持仍显不足。这个现象背后的重要原因是，金融机构和实体企业之间还存在着较为严重的信息不对称，实体经济能够提供的信息，不足以支撑金融的投资决策。因此，需要建立起确保实体产业经营信息向金融机构准确传递的机制，才能推动金融更好地为实体经济服务，实现脱虚向实。利用区块链技术，可以实现“可信数字化”，进而实现实物流、信息流、资金流“三流融合”，则可以有效建立上述机制。

## 5.3 新型平台经济

目前平台经济更多地是“分享经济”，而非“共享经济”模式，平台的使用者与平台的所有者之间存在利益冲突的问题。借助 Token 体系，区块链平台能够将用户对平台或社区的贡献量化并自动结算，给予相应奖励，实现用户与互联网平台所有者共享平台价值的增值。

# 六、 潜在风险

## 6.1 合规性风险

2017 年 9 月，7 部门联合发布《关于防范代币发行融资风险的公告》叫停 ICO，将其定性为非法公开融资并关停国内交易所。 与早期的互联网相似，区块链发展早期也要特别警惕资本市场的过分炒作和虚假宣传。有的项目的所谓创新脱离了实体经济的需求，完全是投机行为。

## 6.2 技术风险

如同任何其他由人类设计的技术一样，区块链不是完美无缺的。

### 6.2.1 底层代码

2018 年 3 月，慢雾安全团队披露了一起由于以太坊生态缺陷导致的亿级数字资产盗窃事件。

### 6.2.2 密码算法

以比特币为例，每个区块都对应一个散列值，采用 SHA256 算法计算得到。在现阶段，该算法依旧满足散列函数的三个特性，单向性、弱无碰撞性和强无碰撞性，是安全的。

比特币中的交易采用了椭圆曲线数字签名算法，椭圆曲线密码并不能抵抗量子攻击，当对于密码的量子攻击在未来成为现实时，所有不能够抵抗量子攻击的密码算法都存在较大风险，需要被替换。

### 6.2.3 共识机制

当前的共识机制有工作量证明（Proof of Work，PoW [BTC]）、权益证明（Proof of Stake，PoS [ETH]）、授权权益证明（Delegated Proof of Stake，DPoS [EOS]）、实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）等。PoW 面临 51%攻击问题。由于 PoW 依赖于算力，当攻击者具备算力优势时，找到新的区块的概率将会大于其他节点，这时其具备了

撤销已经发生的交易的能力。在 PoS 中，攻击者在持有超过 51%的 Token 量时才能够攻击成功，这相对于 PoW 中的 51%算力来说，更加困难。在 PBFT 中，恶意节点小于总节点的 1/3 时系统是安全的。

一旦攻击成功，将会造成该系统的价值归零，这时攻击者除了破坏之外，并没有得到其他有价值的回报。

### 6.2.4 智能合约

若智能合约的设计存在问题，将有可能带来较大的损失。2016 年 6 月，以太坊最大众筹项目 The DAO 被攻击，黑客获得超过 350 万个以太币，后来导致以太坊分叉为 ETH 和 ETC。

2017 年 11 月 7 日 Parity 多重签名合约漏洞导致 93 万个以太币永久丢失。

### 6.2.5 数字钱包

数字钱包主要存在三方面的安全隐患：设计缺陷、钱包中含恶意代码、硬件设备损坏或丢失。