科技参考

（2019 年第 4 期）

区块链技术专题

本期要目

主管：徐州市科学技术局

主办：徐州市科技情报研究所　　2019 年 11 月 5 日

目　录

什么是区块链技术？

10 月 24 日下午，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习。会议强调，要把区块链作为核心技术自主创新的重要突破口，加快推动区块链技术和产业创新发展。

其实，“区块链”并不是今天才出现的新名词，它在 2016 年出现时，就曾吸引科技圈和金融圈目光，一时风头无两，近年来的相关理论研究与技术创新更是向纵深发展。

区块就是很多交易数据的集合，它被标记上时间戳和之前一个区块的独特标记。有效的区块获得全网络的共识认可以后会被追加到主区块链中。区块链是有包含交易信息的区块从后向前有序链接起来的数据结构。

每个区块就像一个硬盘，把以上这些信息全部保存下来，再通过密码学技术进行加密。这些被保存的信息就无法被篡改。

区块链可以通俗地被理解为一个分布式存储的公共账本，这个账本由各个区块连成一个链条。在传统记账系统中，记账权掌握在中心服务器手中。而在区块链这个“账本”上，链条上的每一个点都能在上面记录信息，构成点对点的记账系统。因此，区块链技术被认为是一种去中心化的技术。

用一个简单的例子可以更明了地说明区块链的作用。

比如，在一个 100 人的村庄，张三向李四买了一头牛，向他支付 1 万元。过去，他要依靠中间人赵六，才能将自己的 1 万元转给李四。而有了区块链系统，张三可以直接将自己的 1 万元记到李四的账本上，同时交易信息会传到全村，也就是整个区块链系统，使其他 98 个人也能看到信息。由系统记录整个交易过程，具有可溯源优势，防止赵六账本丢失或李四不认账等问题。

更关键的是，由于以密码学的方法加密，区块链上的数据不能被篡改，保证了信息的可信度真实性。“区块链的核心功能是搭建信任机制。未来，价值的发布、传播等都可能由中心的节点变成每一个人。”有业内人士说。

国家互联网应急中心互联网金融安全技术重点实验室主任吴震表示，区块链技术的核心优势是系统中每一个信息，在网络里多个节点甚至每个节点都保存一遍。“任何节点自行修改数据将不被认可，整个网络因此形成了一张较为严密的大网。”

区块链有哪些特点？

区块链不仅可以记录每一笔交易，还可以通过编程来记录几乎所有对人类有价值的事物：出生和死亡证明、结婚证、所有权契据、学位证、财务账户、就医历史、保险理赔单、选票、食品来源以及任何其他可以用代码表示的事物。

这些总结起来，区块链至少具备以下特征：

第一，分布式存储、去中心化。没有第三方中介，让所有人都有能力都去维护共同一份数据库，通过多地备份，可以有效保证数据存储平稳运营；

第二，信息不可篡改、不可抵赖。一旦进入区块链，任何信息都无法更改，甚至管理员也无法修改此信息；

第三，安全性。所有的数据是分布式存储，都是点对点的，降低了第三方入侵和访问信息内容的风险。即使一个节点被攻击或宕机也不会影响网络的运行；

第四，信息集体维护，具可靠性。网络中的所有节点都可以轻松访问信息，所有人都有能力彼此监督维护数据库的行为，保证数据公开透明，谁也不敢说假话干坏事；

第五，匿名化。区块链是个隐私技术，让数据回归个人，例如，今天我们所有的消费、借款、还款等各种行为是我们个人行为，但个人手上没有数据，数据在银行和商家的系统里。区块链的本质就是让这些数据回归个人，只有个人自己知道，商家或团体可以去做大数据分析，但不知道是哪组数据属于哪个人。

正因为具备这些特点，区块链技术解决了网络世界中最大的难题——信任问题。

我国在区块链方面的发展现状

发布时间：10-3009:35　前瞻网

国家政策大力推动，中国在区块链领域技术竞争优势较大

2016 年，国务院发布《“十三五”国家信息化规划》提出，强化区块链等战略性前沿技术超前布局。这是区块链首次被作为战略性前沿技术被列入规划。此后，一些地方陆续出台推动区块链产业的政策，已有 20 多个省份布局区块链产业。

10 月 26 日中央政治局集体学习，首次明确“区块链核心技术自主创新重要突破口”，意味着区块链的未来发展得到了中央政策层面的高度重视，区块链产业得到正名，有助于正本清源，将对我国区块链技术发展、与实体经济的融合及产业革新起到重大方向性定调的作用。

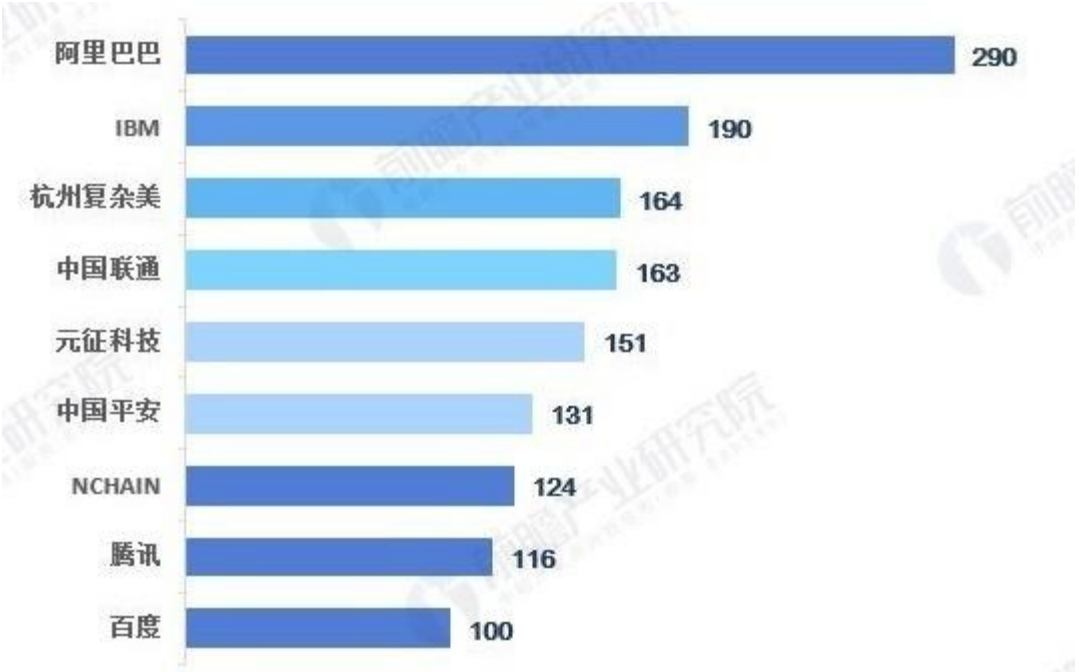
在此次会议中提到，要强化基础研究，提升原始创新能力，努力让我国在区块链这个新兴领域走在理论最前沿、占据创新制高点、取得产业新优势。

“最前沿”“制高点”“新优势”，三个词明确地说明了我国在区块链竞争领域的目标：争夺第一。

2019 年区块链技术专利数量中，我国企业优势明显

目前，全球范围内，企业看，区块链技术竞争已经形成了第一梯队和第二梯队，截至 2019 年 4 月，阿里巴巴以 290 件区块链专利，排在 2019 上半年全球区块链专利排行榜榜首。同时观察第一梯队、第二梯队的企业，发现他们均来自中国。整体看，中国互联网公司在区块链的技术积累较为深厚。中国在区块链领域技术竞争优势较大。

图为：2019.1 月-4 月全球区块链专利排行榜第一梯队（单位：件）



区块链技术未来六大发展趋势

随着我国区块链技术的不断发展，区块链应用领域的不断拓展，未来我国区块链行业将呈现区块链成为全球技术发展的前沿阵地，开辟国际竞争新赛道；区块链领域成为创新创业的新热土，技术融合将拓展应用新空间；区块链未来三年将在实体经济中广泛落地，成为数字中国建设的重要支撑；区块链打造新型平台经济，开启共享经济新时代；区块链加速“可信数字化”进程，带动金融“脱虚向实”服务实体经济；区块链监管和标准体系将进一步完善，产业发展基础继续夯实。

随着国家出台相应文件对区块链进行规范，区块链行业将会从野蛮生长的阶段进入一个规范化发展新的时代。

区块链技术未来怎样发展

虽然已经开始探索区块链在物联网、智能制造等领域的应用落地，但总体看，由于涉及场景较为复杂，落地模式还不够清晰，区块链在实体经济领域的应用还处于起步阶段，还须完善技术，找准应用场景，解决工程实施等现实难题。

工信部信息化和软件服务业司有关负责人表示，将着力于推动区块链和工业互联网的融合发展，推动制造业加快数字化转型步伐；推动区块链和大数据的融合发展，利用区块链技术探索数字经济模式创新；把区块链作为核心技术自主创新的重要突破口，着力推动区块链技术产业创新发展，带动软件和信息技术服务业做大做强；促进产融结合，引导资本赋能实体经济，促进大中小企业融通发展。

值得注意的是，在区块链的一些应用中，所有交易数据都是公开透明的。因此，信息隐私如何保障，是区块链发展须解决的课题。专家建议，要加强对区块链技术的引导和规范，加强对区块链安全风险的研究和分析，探索建立适应区块链技术机制的安全保障体系，推动区块链安全有序发展。

业内人士认为，不断加强基础技术理论的研究和突破，区块链才能安全、可靠、持续的发展与应用;不断完善基础支撑设施，区块链应用的落地才能有序健康。一方面，要加强相关基础技术理论的研究，例如与区块链性能和安全相关的共识算法、与数据隐私相关的零知识证明等密码算法;另一方面，需加快完善基础支撑设施的建设，如区块链行业公共网络、分布式数字身份体系等。

北京大学(天津滨海)新一代信息技术研究院金融科技研究中心主任董宁认为，要重视区块链技术的标准并加以推广。“建议在区块链技术产业落地过程中，让更多企业参与行业应用标准化研究，进而形成国家和国际标准，提升我国在该领域国际话语权和规则制定权。”

区块链技术竞争初现 阿里巴巴专利申请位居榜首

2019-10-06 16:00:43　　来源：前瞻产业研究院

2018 年区块链发展概况

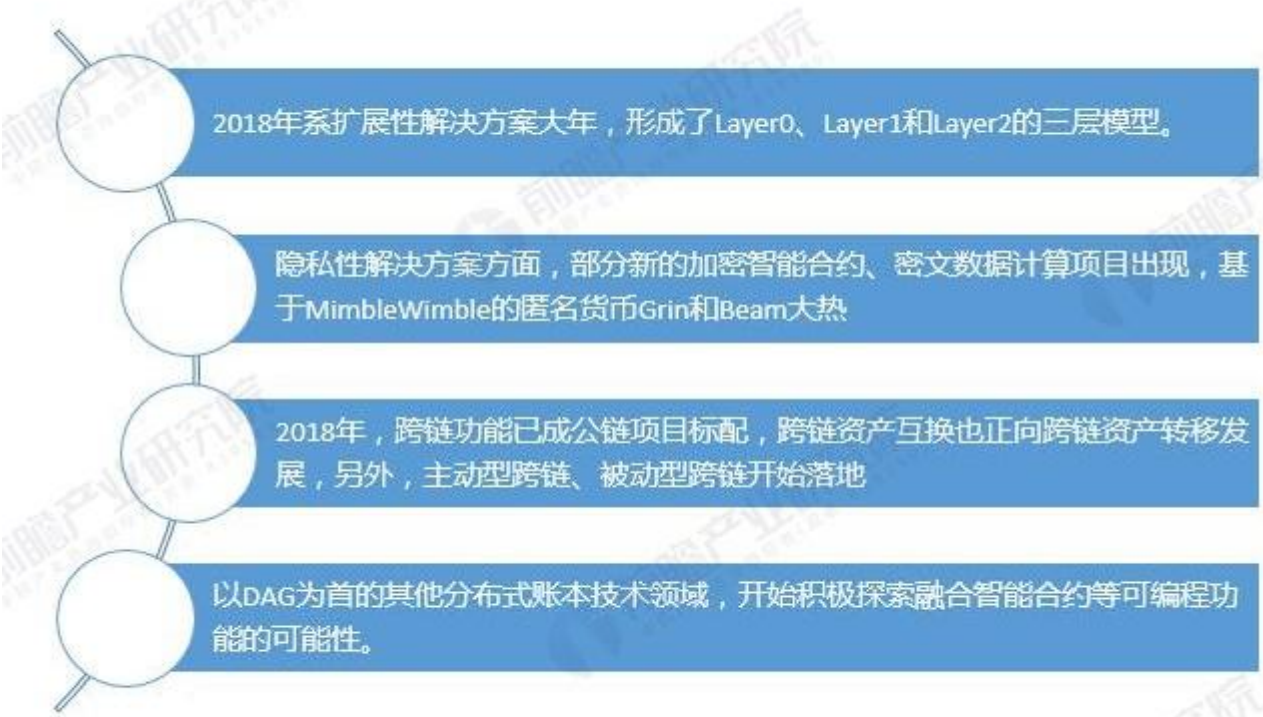
2018 年系数字资产市场由狂热到理性的一年，二级市场各项数据均大幅下滑，并传导至一级市场。同年，比特币链上活跃度亦大幅下跌。但算力、挖矿难度等核心指标依旧健康。这样的市场环境也进一步传导向区块链市场，整体来看，区块链市场喜忧参半。首先在产业板块领域，硬件与基建层发展不理想、平台与基础层发展回归理性。但技术发展迅猛同时各国正在从构建信任、数据自治与价值化及通证激励等领域努力，从而推动技术商业化应用落地。

图表1：2018年区块链市场发展概况

资料来源：前瞻产业研究院整理　　@前瞻经济学人APP

技术发展上看，共有以下四个成果——(1)2018 年系扩展性解决方案大年，形成了 Layer0、Layer1 和 Layer2 的三层模型;(2)隐私性解决方案方面，部分新的加密智能合约、密文数据计算项目出现，基于 MimbleWimble 的匿名货币 Grin 和 Beam 大热;(3)2018 年，跨链功能已成公链项目标配，跨链资产互换也正向跨链资产转移发展，另外，主动型跨链、被动型跨链开始落地;(4)以 DAG 为首的其他分布式账本技术领域，开始积极探索融合智能合约等可编程功能的可能性。

图表2：2018年区块链技术发展概况



资料来源：前瞻产业研究院整理　　@前瞻经济学人APP

故整体看，2018 年区块链技术发展较为迅猛，但硬件市场、公链市场发展差强人意。

2019 年投资概况

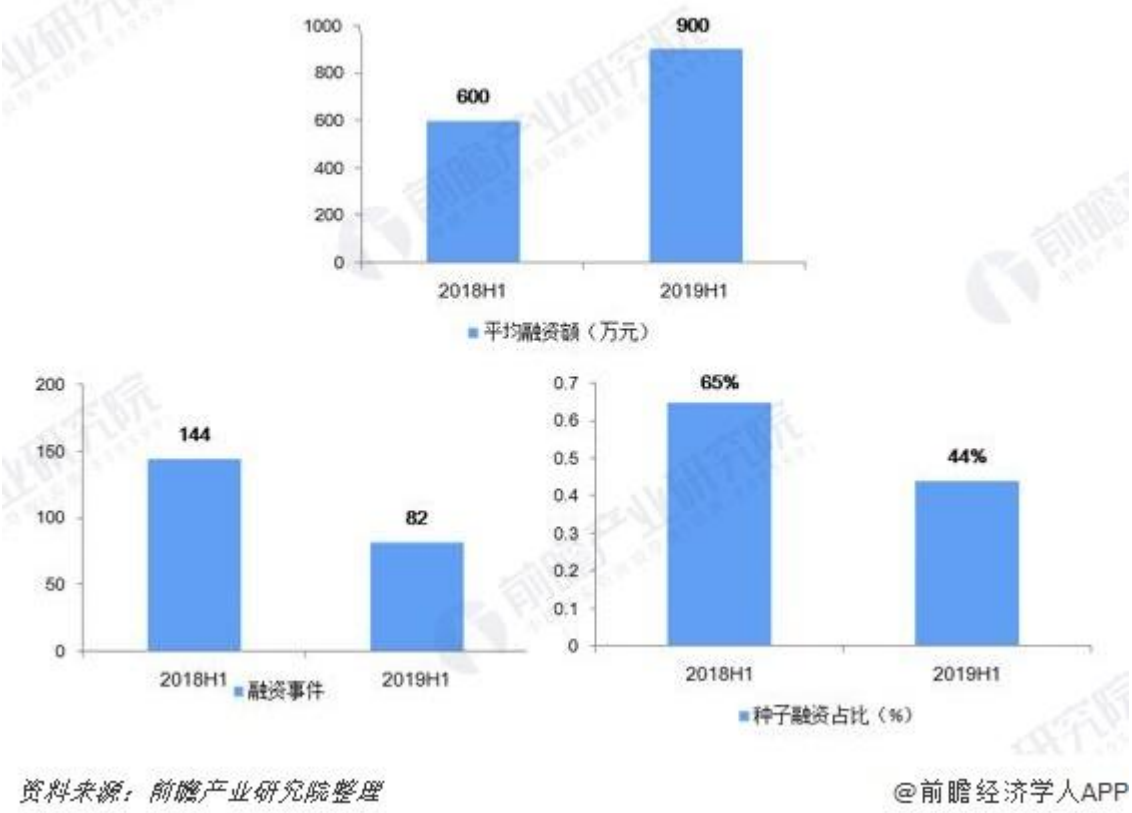
2019 年 9 月 17 日，在上海区块链周第五届区块链全球峰会上，普华永道亚州金融科技咨询顾问 LucyGazmararian 发布了《普华永道全球区块链并购及融资报告》。

报告中显示，从融资类型和规模来看，2018 年上半年总成交数 144 笔，投资金额约 600 万美元，2019 上半年总成交数 82 笔，投资金融同比涨幅 50%，达到约 900 万美元。但 Lucy 表示，区块链行业的投资规模仍然较小。同时，2019 年和 2018 年在投资类型分布上并没有特别大的区别，都是种子轮占最大比重，

但可以看到2019年上半年种子轮占比同比有所下降，从65%下降到44%，同时2019年上半年A轮和B+轮的占比同比略微上升。

数据可知，2019年上半年区块链延续了2018的发展概况，投资降温。

图表3：2018.06-2019.06世界区块链投资概变动(单位：万元，件，%)

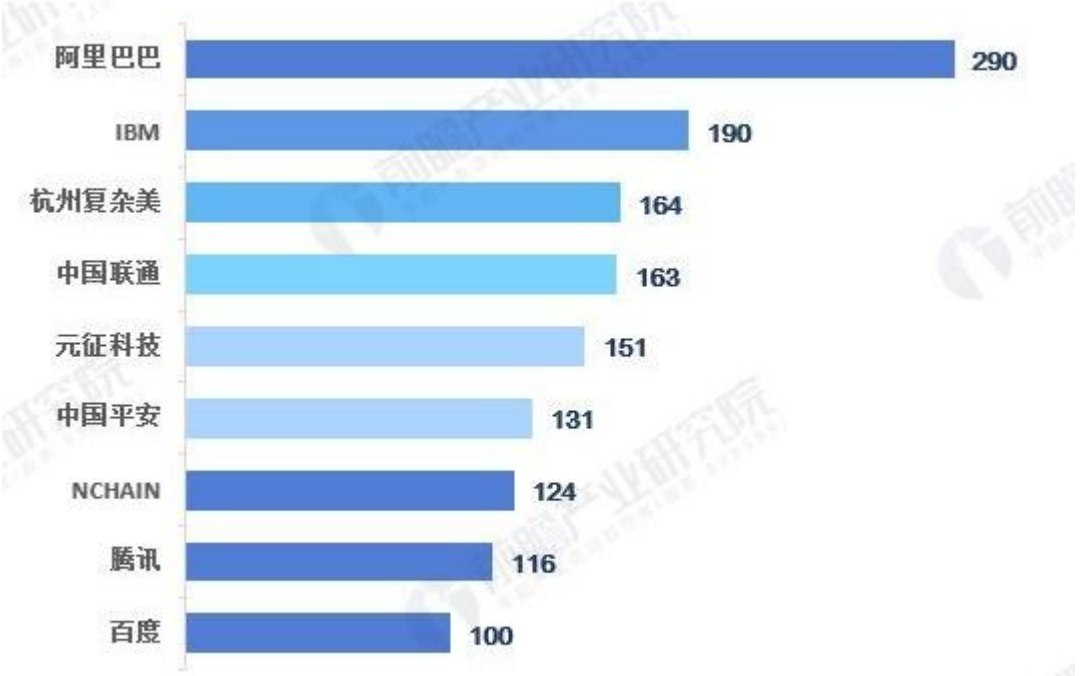


资料来源：前瞻产业研究院整理　　@前瞻经济学人APP

2019年区块链技术专利申请概况

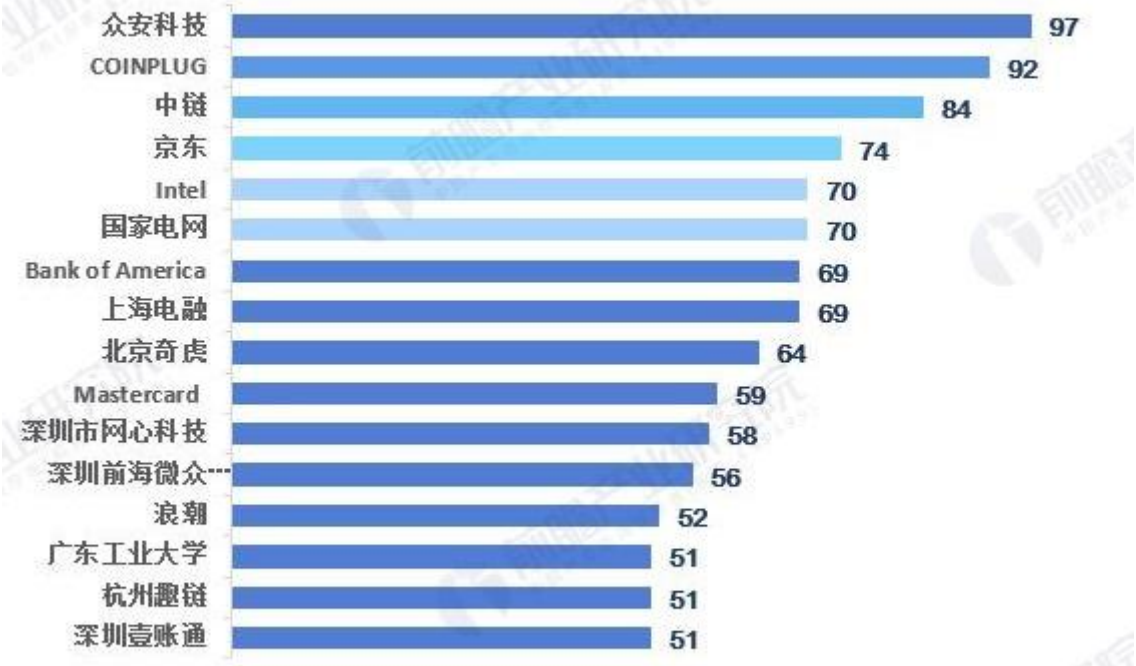
目前，全球范围内，企业看，区块链技术竞争已经形成了第一梯队和第二梯队，截至2019年4月，阿里巴巴以290件区块链专利，排在2019上半年全球区块链专利排行榜榜首。同时观察第一梯队、第二梯队的企业，发现他们均来自中国。整体看，中国互联网公司在区块链的技术积累较为深厚。中国在区块链领域技术竞争优势较大。

图表4：2019.01-04全球区块链专利排行榜第一梯队(单位：件)



资料来源：前瞻产业研究院整理　　@前瞻经济学人APP

图表5：2019.01-04全球区块链专利排行榜第二梯队(单位：件)



资料来源：前瞻产业研究院整理　　@前瞻经济学人APP

2019 年区块链市场规模

在市场规模上，预测期内美国仍是全球区块链投资最大的区域，占全球支出的比重为 36%。分列二到五位的是西欧、中国、亚太(不含中国和日本)和加拿大。从垂直行业规模来看，银行业仍是全球区块链支出的第一大行业，其次是离散制造、流程制造、零售和专业服务行业，前五大行业区块链支出占全部支出的比重达到 58.4%，行业分布较为集中。在应用场景上，跨境支付和结算、产品溯源、贸易金融及交易(后)管理、资产和货物管理、身份认证等排名较为靠前，其 2018 年全球市场支出均在 1 亿美元以上。

而根据 Tractica 的一份新报告，这种自动化和加密技术的结合产生了各种各样的企业用例，这些用例对各行各业都十分具有吸引力。2018 年全球企业区块链市场在 46 亿美元左右，到 2025 年这个数字将达到 203 亿美元。

图表6：2017-2025年全球区块链市场规模(单位：亿元)

资料来源：前瞻产业研究院整理　　@前瞻经济学人APP

2019 年区块链投资机会

经过研究分析，前瞻认为，2019 年的区块链市场将在以下领域存在投资机会

第一，区块链领域的并购活动将增加，企业倾向直接购买相关业务，而不是发展原生区块链业务。2018 年挖矿行业的并购业务最活跃，但到了 2019 年，区块链基础设施领域的并购最活跃。第二，区块链领域的融资活动将增加。融资活动最活跃的三大细分领域区块链基础设施、交易基础设施和交易所持续活跃，但有交替变化。第三，行业的参与机构持续扩大，比如摩根、中国建行、facebook、微软等。

2018 年中国区块链行业发展现状分析

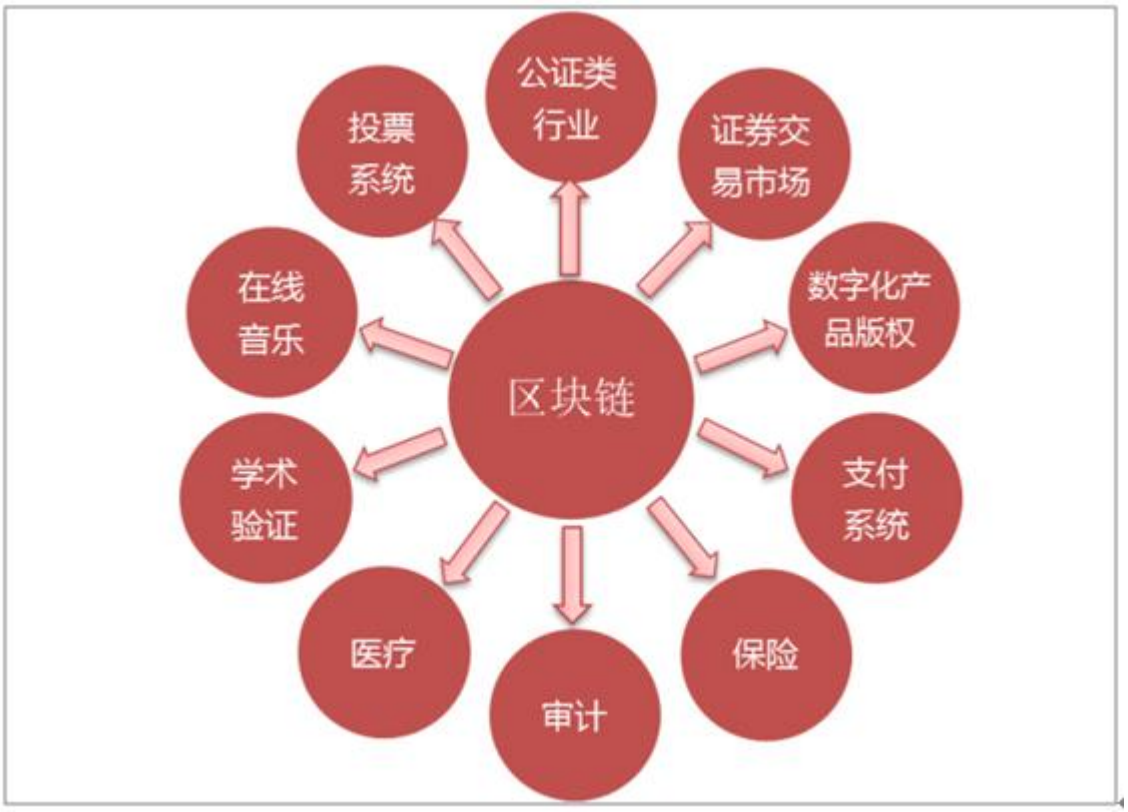
2019 年 10 月 09 日 13:26:09

区块链行业有望基于平台和生态快速增长

区块链是一种可信的数据处理和存储技术，具有区块+链式数据结构和分布式存储架构。区块+链式的数据结构是指将一段时间内的多个交易信息打包成一个区块，计算区块的摘要信息（哈希值），然后与上一个区块的摘要信息组合在一起，形成新的区块。以此类推，这些区块通过摘要信息链接起来，形成了区块+链式的数据存储结构。

区块链早期是由技术极客驱动行业发展，但当前区块链面临的最大挑战是如何结合应用场景落地。市场上有大量企业在多个领域进行了若干探索，目前已有一些场景可以用区块链解决行业实际问题，其中以金融相关场景的应用落地最为广泛。

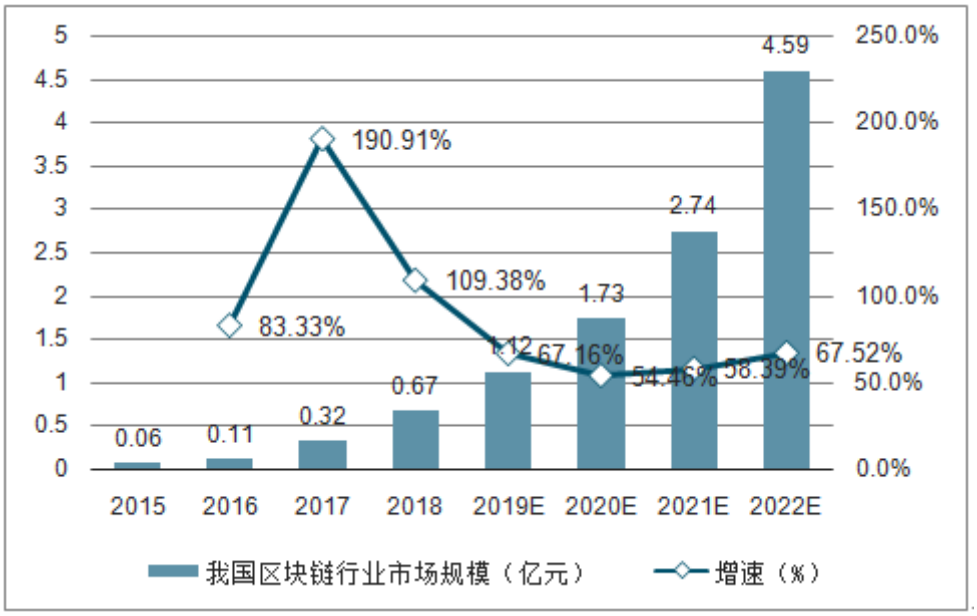
区块链可应用于多个场景



截止 2018 年我国区块链行业市场规模已经达到了 0.67 亿元，始终保持 80%以上的速度飞速增长。预测 2019 年我国区块链行业市场规模将突破 1 亿元，并预计在 2022 年，在政策支持和下游需求的推动下，我国区块链行业市场规模有

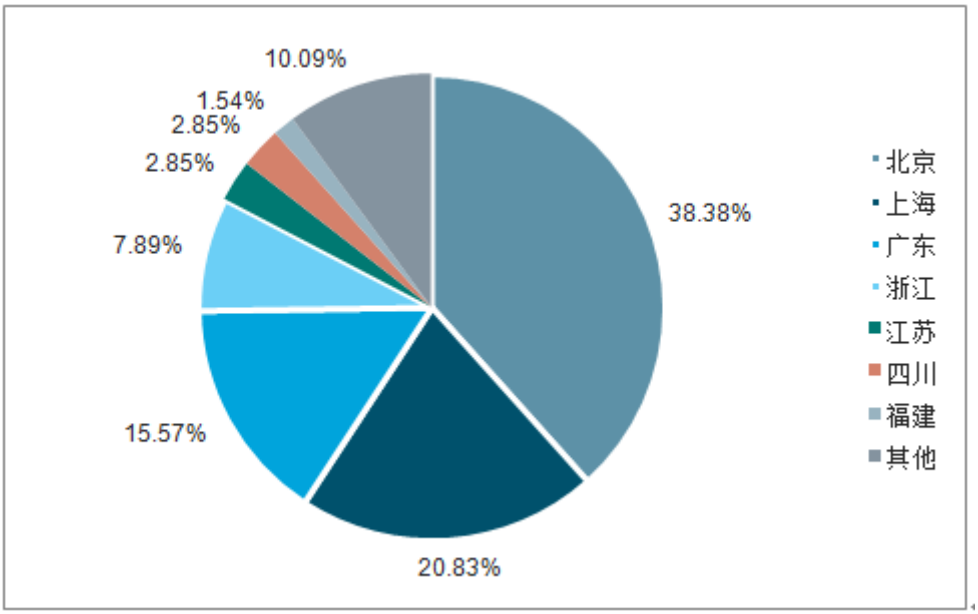
望突破 4.5 亿元。

2015-2022 年我国区块链行业市场规模统计及增长情况预测



我国以提供区块链技术或服务为主营业务的公司已经达到 456 家，产业初步形成规模。区块链公司地域分布相对集中，产业集聚效应明显，北京、上海、广东和浙江是区块链行业创业的集中地，四地合计占比超过 80%。其中，北京以 175 家公司，占比 38.38%处于绝对领先地位;上海以 95 家公司，占比 20.83%位居第二;广东以 71 家公司，占比 15.57%排在第三。除此以外，中国区块链行业活跃度前十地区还包括浙江、江苏、四川、福建、湖北、重庆和贵州。

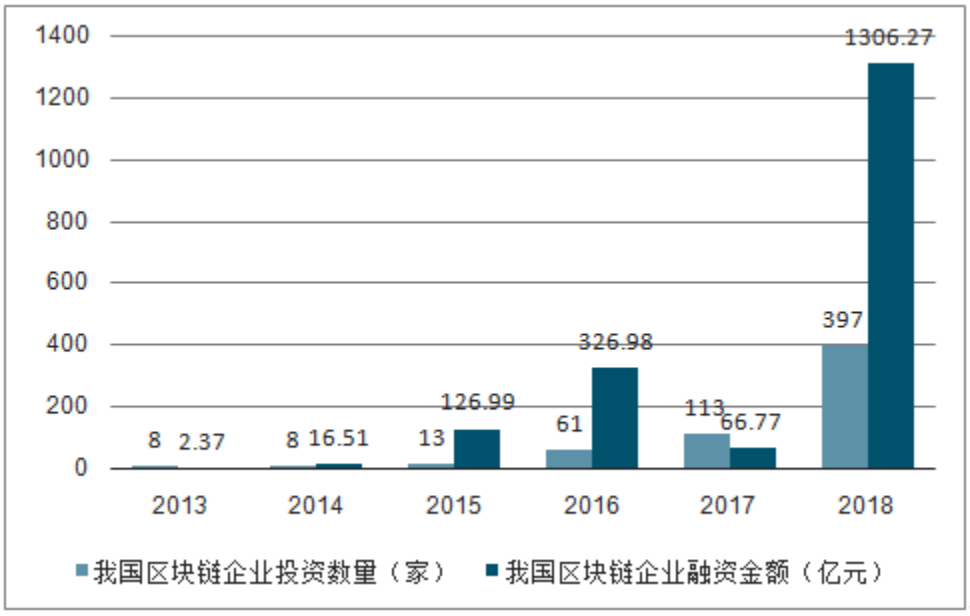
2018 年中国区块链企业地域分布占比统计情况



2013-2018 年，我国区块链相关企业获得投资数量以及融资规模均呈不

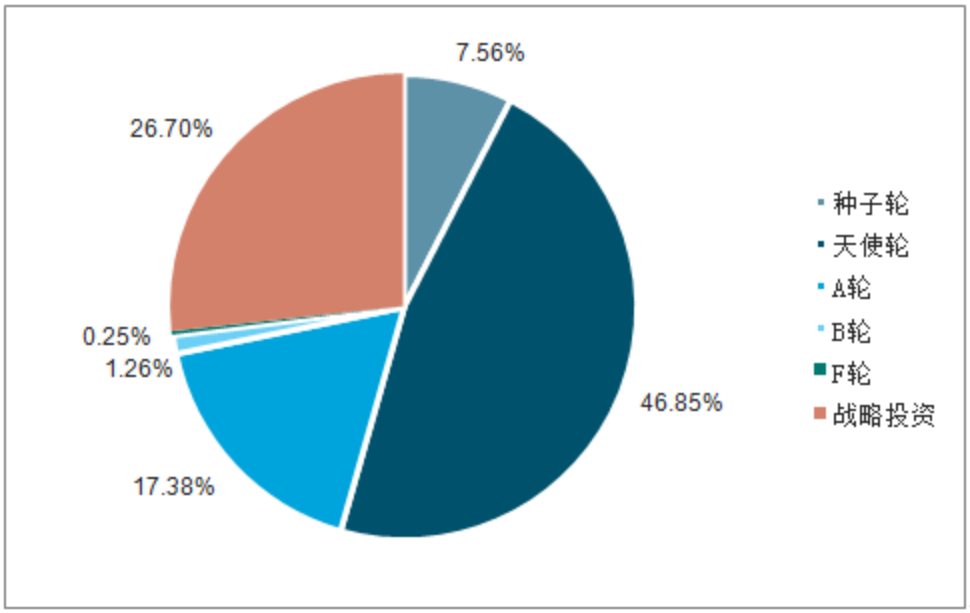
断上升趋势，2018 年，区块链相关企业获得投资呈现爆发式增长，获投企业数量由 2017 年的 113 家增长至 397 家;融资金额从 2017 年的 66.77 亿元增长至 2018 年的 1306.27 亿元。

2013-2018 年我国区块链企业投资数量、融资金额统计情况



从投资轮次来看，我国区块链行业整体还处于初级阶段，融资轮次也以 B 轮以前居多。2018 年，我国区块链相关企业共计发生 397 起投资事件，其中种子轮 30 起，占据全部投资事件的 7.56%;天使轮 186 起，占据全部投资事件的 46.85%;A 轮(包括 Pre-A、A 轮、A+轮)共计 69 起，占全部投资事件的 17.38%;B 轮以前的投资事件合计占比超过 70%，融资多数处于初级阶段。

2018 年我国区块链行业投资轮次占比统计情况



目前区块链已经走出了行业早期的泡沫阶段，应用场景逐步开始落地。由于区块链作为可信基础设施的潜力，全球的金融机构、科技公司、监管部门一直都高度关注区块链行业的发展机遇，未来一旦商业模式大规模落地，有望基于平台和生态快速增长，形成远大于现有互联网巨头的生态。未来空间巨大，看好行业发展。

区块链如何赋能数字经济？

发布时间：10-3009:47 东方财富信息股份有限公司

然而，尽管区块链技术如此伟大和革命性，但区块链本身在很多领域仍然限于一种理想和思潮，当前真正落地的应用并不多。从国内外来看，落地较为成熟的应用主要还是在数字货币等金融领域。

目前的主要应用案例包括：在跨境汇款领域，蚂蚁金服利用区块链技术为中国香港，以及菲律宾、巴基斯坦、马来西亚等一带一路沿线国家提供低费率，高速的跨境汇款服务等。

在清结算领域，港交所计划利用区块链结算系统简化互联互通下内地股票的北向交易流程，方便欧美投资人投资 A 股。

区块链技术应用的真正突破和落地尚需时日。那么，未来除了金融领域，区块链技术还可能会应用在哪些场景？

一是数字身份。我们现在远行或出门办事，总是要提供各种证件，目前，如出生证、房产证、婚姻证都需要一个中心节点，部分证明在跨出国门就失去了公信力，因为其缺少一个全球性的中心节点。

但区块链的去中心化和不可篡改性可以从根本上解决这一问题，有了区块链，就不用担心找不到证件来证明“我就是我”的问题；

二是医疗卫生。如，一个人的病例可以用区块链来管，如医生看病，个人可以医生授权看到病例，但医生甚至可以对不上是哪个人；在区块链平台中，利用区块链建立有时间戳的通用记录存储库，进而达到不同数据库都可提取数据信息的目的。这样一来，患者就无需再在不同医院进行反复检查，也无需再为报销医保反复折腾，节省了看病时间，对于时间就是生命的医疗行业来说，区块链意义重大。

三是公共管理。主要是食品安全溯源、药品溯源等应用；

四是知识产权保护。专业人士自己的作品放在区块链上，有人使用了他的作品，他就能立刻知道。相应的版税也会自动支付给创作者。区块链技术既保护了版权，也有助于创作者更好更直接地向消费者售卖自己的作品，而不再需要发

行公司的协助。

五是供应链管理。在基于区块链的供应链管理体系中，记录存储和溯源都是很容易的,因为企业的信息可以通过内置感应器和RFID标签来获得产品信息。产品从起源地到终点所在的过程都可以通过区块链来追踪。而且，这类准确的溯源方式，可以用来检测供应链中的缺陷。

更便捷的交易

由于没有第三方的参与，区块链可以让支付和交易变得更高效、更便捷。同时区块链平台也允许用户创建在满足某些条件时变为活动的智能合约，这意味着当交易双方同意满足其条件时，可以释放自动付款。降低交易门槛，提高交易流通的效率。

例如我们经常会用携程、美团等 app 来寻找并下单入住酒店和其他服务，各个平台从中获得提成。而区块链的应用正是除去中间商，并为服务提供商和客户创建安全、分散的方式，以达到直接进行连接和交易的目的。

此外，在贸易、慈善等诸多领域，也是区块链技术的应用场景。

由此可见，从比特币开始的区块链 1.0，到如今区块链 3.0，区块链技术从仅仅应用于加密货币支付、流通的程度，已经逐渐演变成如今能在社会领域下，实现场景应用，为各种行业提供去中心化解决方案。

尽管如此，我们也要警惕，在区块链解决人类过去信任和安全问题的同时，其本身也产生了极大的信任和安全问题。对于区块链技术的监管还需要各方的合力。

澳大利亚发布国家区块链战略路线图

2019 年 04 月 16 日 15:33:40

3 月 18 日，澳大利亚公布了国家区块链战略路线图（National Blockchain Roadmap），并增加了 10 万澳元的联邦政府资金。澳联邦工业、创新和科学部长安德鲁斯和贸易、旅游和投资部长伯明翰联合表示：“新的区块链战略路线图旨在促进澳成为新兴区块链产业的全球领导者”。

该路线图将加强对区块链产业的监管引导、技能培训和能力建设，加大产业投资力度，增强国际合作，提升产业竞争力。政府将强化与来自工业界和学术界的区块链技术专家以及澳联邦科工组织（CSIRO）Data61 小组的密切合作，将

区块链整合到政府和金融部门，加快政府的数字化转型，确保澳在该技术领域保持领先地位。该笔 10 万澳元的资金将用于资助澳公司参加澳贸委会于 5 月在纽约举行的区块链投资会，帮助澳区块链公司和初创企业与投资者和客户建立密切联系。

澳总理斯莫里森在 2018 年曾向数字化转型局（Digital Transformation Agency）提供了 70 万澳元的资金，以促进政府部门利用区块链技术向数字化转型。同年 7 月，IBM 与澳政府签署了一项为期 5 年价值 10 亿澳元的协议，该协议将使用区块链和其他新技术来改善政府部门的数据安全。

数字货币有多大可能性？

2019-10-29 09:15:55　　来源：智本社，作者：清和社长

人性，总是依赖安全，又追逐自由！

比特币不是莫名其妙蹦出来的“妖猴”。从技术上讲，几十年前技术精英选择了中心化数据库，今天成就了高效、稳定、庞大的 FACEBOOK、谷歌、微信等巨无霸平台。

然后，我们现在开始想要追逐自由了。想要数据私有权、数字资产私有权，享有私有权才有自由，才有隐私权和收益权。

同时，我们呼唤安全，虽然分布式账本未必比中心化数据库更加安全，但是前者是信任自己和代码，后者是信任他人和权威，人性上讲显然更倾向于选择前者。

从货币上讲，除了哈耶克等少部分自由主义者质疑过法定货币垄断权问题，大部分人还是默许了这一存在，或许没能找到更好的解决方案。拨开云雾看本质，你会发现，比特币其实还不能算是一种货币，其发行机制上的缺陷是致命的。但是，比特币给世人打开了潘多拉魔盒。

数字货币，是目前区块链唯一一个成熟的应用场景。研究区块链，定然离不开比特币和数字货币。

货币的本质是什么？

一切还得从 2008 年金融危机说起。

若 1929 年那场大危机及大萧条让世人看到了市场的脆弱性，那么，2008 年这次金融危机则暴露出了政府干预主义的危害。更令人无奈的是，危机爆发后，

美国联邦财政部及美联储又以人为干预的方式救市。

当时，美联储主席伯南克推行第一期量化宽松，决定购买3000亿的美元长期国债、收购房利美与房地美发行的大量的抵押贷款支持证券。

就连凯恩斯都知道，货币扩张，会引起财富重新分配，而使一些阶级得益，另一些阶级受损。

这时，一群技术极客忍不了了。2008年12月，一个代号为“中本聪”的人发布了《比特币白皮书——一个点对点的电子现金系统》。

“中本聪直指法币的要害：“传统货币的根本问题就是，它们必须得到全部的信任才能发挥作用。必须信任中央银行不会使货币贬值，然而历史上却不乏违背这一承诺的情况……”

2009年1月3日，比特币网络第一个区块被挖出时，中本聪在嵌入文本中批判：“财政大臣站在第二次救助银行的边缘”。

当时，中本聪将矛头指向币权垄断、货币贬值、美元霸权，试图取而代之。

于是，比特币诞生之时，就裹挟着一种“信仰”：分布式、民主化、自由化，反特权，反货币霸权。

中本聪的野心不仅仅是发布一种私人货币（竞争性货币），而是建立“一个点对点的电子现金支付系统”。所以，比特币背后至少包含三层含义：

一是比特币是非法定、无国界货币，即货币的非国家化；

二是比特币网络是一个去中心化的分布式网络，一个无国界的银行转账及支付系统；

三是比特币的出现，意味着一种非国家化的超主权货币以及无国界金融体系的尝试。

从历史来看，货币非国家化的历史，要远远长于法定货币。经济学家韦伯将这种“没有国家的保障”、由习俗或契约支撑的货币，称之为“卡尔塔货币”。日本黑田明伸教授将这种局部人认可并发行的货币，称之为交手货币，也叫“支付协同体”。

最为典型的例子莫过于金银。金银在很长一段时间都是世界通用的货币，各国商贸的硬通货，不属于任何一个国家。即使在金本位时代，国家发行法定纸币，但法定纸币依然是以自由竞争的黄金为锚，黄金在全球自由流通，且比纸币更为硬通。

早期人们使用的贝壳、铁钉、食盐、石币、金银、银行券都不是国家化的，都是市场自发形成的。比如银行券是早期威尼斯、伦敦等城市的私人金铺向客户

发行的“凭证”。

历史上，黄金、白银、银行券都不是法定货币，货币的非国家化的时间远远大于国家化。

根据货币的本质——货币即合约，货币的非国家化在历史上、理论上都站得住脚，比特币、以太坊、Libra 稳定币以及私人货币，至少具有“合理性”。

弗里德曼好友张五常先生，自称对货币理论并不精通，但他却一语道破货币的天机——“一纸钞票或一纸支票，皆合约也。”

不管是羊皮、金银、香烟、铁钉、大米、石币，还是金本位货币、纸币，货币都是市场的共同契约，即交易解决方案——降低交易费用。古代，金银货币稀缺，地租与农民约定用大米来缴纳地租，这时大米既是资产又是交易媒介。

所以，货币是一种在市场交换中主体自发认可的“看不见的协议”。本质上，所有的货币都是协议本位。

美元是美国人的合约，欧元是欧元区国家的合约，数字货币是数字货币持有者的合约。合约，数字货币支持者一般理解为“共识”，执行合约叫“记账”。

比特币是比特币支持者们的合约，以太坊是以太坊支持者们的合约，Libra 稳定币是 Facebook 支持者们（27 亿全球潜在用户）的合约。

比如以太坊是典型的合约货币。以太坊有一个创新，那就是智能合约，开发者可以利用智能合约开发 Dapp，支持者们可以使用以太坊投资、消费 Dapp。这就是“以太坊”这一共识货币的应用场景。

以上货币即合约的主张，论证了货币的非国家化的合理性。

数字货币能否成功？

不过，并不是一群人制定了一个交易合约，它就自动会成为货币。

不管是市场自发形成的协议，还是群体、国家协商制定的合约，目的都是为了确定一个可靠、可信的交易媒介（货币）。何为可靠、可信？

除了质地均匀、不易腐烂、便于携带、易于切割外，最根本的是价格（价值）稳定。没有任何一个国家、群体会使用一种不稳定的媒介作为货币。历史上，没有任何一种不稳定的货币能够长久。所有的货币都崩溃于大幅度贬值，或相对价值不稳定。

所有货币合约中，都有一条“使命性质”的义务：货币价格稳定。

币值稳定，是货币的灵魂。只有价格稳定，货币才有信用，人们才敢持有这种货币。反之，人们避之不及，甚至一文不值。

所以，货币当局（发行方）最根本的义务就是维持货币价格的稳定。

反过来，如果货币价格不稳定，尤其是大幅度贬值，就相当于货币当局违反合约、背弃承诺。

张五常先生在《经济解释》中一针见血地指出：“从合约的角度看货币是重要的，而这样看，通胀或通缩的出现算是毁约……我们听到的要求稳定物价的声浪其实是要求守约。”

再看比特币、以太坊和 EOS，这些数字货币的价格涨跌幅度都非常大，价格极度不稳定，本质上是违背了货币合约，致使其丧失了货币的交易功能属性。他们从此与货币渐行渐远，彻底变成了投机性数字资产。

主要原因是，数字货币这种合约中，即“白皮书”，在发行机制上存在巨大缺陷：

首先，比特币、以太坊、EOS 强调去中心化，没有货币发行的责任主体。换言之，没有一个类似于央行的机构来维护货币价格的稳定。

其次，比特币是一个封闭的、与市场隔绝的发行机制，无法维护货币价格的稳定。

中本聪表达了对传统银行系统的不信任以及货币超发的不满，试图通过定额发行（2100 万枚）的方式维持比特币不贬值。实际上，这种办法是机械的、无效的。

货币不是为了发行而发行，货币的功能是服务于市场交易。货币不应该定额发行，而是按市场需要发行。中本聪采用定额发行机制，试图让比特币不断升值，结果却适得其反。

最后，以太坊、EOS 注重货币应用场景，但忽略了价格稳定的重要性。

以太坊的智能合约推动了 Dapp 的发展，也为以太坊这一货币找到了一个很好的应用场景。很多人购买以太坊投资项目，项目方也乐于收取以太坊。但是，当以太坊价格大幅度下跌时，这一美好的应用场景就崩溃了。

2018 年下半年每当比特币下跌时，以太坊跌得更加凶狠，尤其是比特币跌破 6000 美元关键支撑时，以太坊大幅度杀跌。原因就是大量项目方抛售以太坊发生集体踩踏，他们抛弃以太坊换回美元以稳定财富值。

如何才能维持货币价格稳定？何种货币合约才可信？

从人类货币史来看，大致有几种解决办法：

在商品和金属货币时代，最朴素、最原始、最常用的办法就是选用靠谱的商品或金属。比如岛民偏好石币，渔民偏好贝壳，游牧民族偏好羊皮，古代中国使用铜钱。

在金本位时代，以黄金作为基础发行，以稳定货币价格。

到了信用货币时代，货币不能与黄金刚性兑付，货币价格的稳定依托于制度安排，即对货币总量的控制机制，以及公开市场、利息等调节手段。

信用本位替代金本位，实际上是回归了货币的本质——一种纯合约本位货币，不需要商品、黄金兜底，仅依靠制度安排。

具体做法是，央行以证券、债券、外汇作为储备资产发行货币；当货币价格下跌或上涨时，通过买卖证券、国债、外汇储备等资产来回收、释放本币，以维持本币价格稳定。

但是，比特币、以太坊、EOS 都没有这种发行机制，当价格下跌时，发行方没有任何资产如外汇、证券能够回收这些货币以维持价格稳定。

货币发行面临一个问题：谁能够获得货币。比如，在金本位货币时代，持有黄金的人可以换得货币。在信用货币时代，持有土地、房地产、国债的人容易在银行获得贷款。

货币发给不同的人，对经济的作用也是不同的，同时财富分配结果也是不同的。越接近货币发行权的人越容易获得财富。在信用货币时代，货币超发其实有利于持有房地产、股票、国债的富人。这就是坎蒂隆效应。

中本聪认为这是不公平的，货币发行应该是公平的。怎么才能做到公平呢？

中本聪想了一个办法，那就是平等竞争、多劳多得。

所以，比特币的发行机制叫工作量证明(Proof Of Work，简称 POW)的共识算法。所谓“共识算法”就是协议里具体的权力、义务及规则。工作量证明则是按照哈希运算效率来竞争记账权。

具体做法是，中本聪出一道数学题，解哈希函数，即“在自己的区块中找到一个具有足够难度的工作量证明”。当然这个工作由计算机来完成，算力越强的计算机，竞争胜出的机会越大。这样算力超强的专业矿机就诞生出来了。

胜出者可以获得这个区块的记账权。当全网广播和其它节点确认后，你就可以将这些转账记录在区块之中，然后“跟随该区块的末尾，制造新的区块以延长该链条”。这个过程就叫“记账”，这个链条就是区块链。这就是一个分布式的账本。

这个记账过程是公开的、平等的、不可逆的，被认为是更加可信的。这就是区块链的价值。

但是，如果没有好处，谁愿意干记账工作？

每赢得一个区块记账权，都有若干个比特币奖励。

所以，你的权力和义务是记账，你的收益则是比特币奖励。挖矿实际上是为了争夺记账权，比特币（作为货币）实际上是为了驱动比特币区块链网络而设计的奖励机制。

挖矿和记账的整个过程，其实也是比特币基础货币发行的过程。这个过程看起来比较公平，但是它忽略了最重要的一点，那就是没有资产储备。

本质上来说，比特币是劳动本位或叫电力本位，但是劳动和电力被消耗了，但比特币网络却没有增加任何如证券、债券、黄金之类的资产。没有资产的结果不是比特币不值钱，而是无法通过买卖资产来维持比特币的价格。

这导致比特币完全违背了货币合约，比特币价格波动剧烈，失去了货币价值。

所以，比特币、以太坊、EOS 以及大部分数字货币，都失去了货币的价值，都违背了货币的合约。

不过，Facebook 的稳定币 Libra，规避比特币发币机制上的弊端，采用了 EOS 超级信用节点的优势，结合了现代货币制度——以一篮子货币为储备资产，是一个相对完善的数字货币合约。

Libra 最初由美元、英镑、欧元和日元这 4 种法币（可能还包括新加坡元）计价的一篮子低波动性资产作为抵押物。Libra 可以通过买卖美元、美债等方式维持其价格稳定。这样 Libra 有条件履行其货币合约，成为真正意义上的“货币”。

所以，只要解决价格波动的问题，未来私人货币存在是极有可能的。

不过，Facebook 的野心不仅仅是一个跨国界的私人货币。Libra 白皮书开篇便霸气侧漏：“Libra 的使命是建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施。”

何为央行数字货币？

不少国家的央行都对数字货币的兴起颇为浓厚，市场一直在猜测中国央行是否会推出数字货币。

首先，要解释一个疑点，很多人认为现在的电子货币不就是数字货币吗？其实不是，现在的电子货币是货币数字化，而不是数字货币。

货币数字化和数字货币在债权性质上存有根本区别：货币数字化是 M2，属于商业银行的负债；数字货币是 MO，属于央行的负债。

数字货币的出现，或许改变货币市场结构，增强央行的货币控制力。数字货币时代虽然基本上消灭了现金，但是 MO 却回来了，数字货币与现金一样都是 MO，属于央行的负债。

根据中国人民银行姚前博士公开的信息，央行数字货币拟采用“双层架构”，即银行账户加数字货币钱包账户。数字货币钱包账户实际上是映射到商业银行系统的个人“钱包”，属于MO范畴。银行账户系统里的资金属于M2范畴。

不过，央行数字货币不可能是一个分布式的账本。它更像是在现有的银行系统中加入了一个中心化的钱包系统，可以简单理解为央行系统下开设了一个可以不需要跨行、点对点转账的无息账户，以存放电子现金。

知识拓展——

区块链≠比特币

发布时间：10-3009:47 东方财富信息股份有限公司

必须指出的是，区块链不是今天才兴起的。自 2007 年，传说中的日本人中本聪开始探索用一系列技术创造一种新的货币--比特币，作为支撑比特币基层技术的区块链就进入人们的视野。以至于到今天，很多人把区块链等同于比特币。

实际上，比特币刚诞生时并没有“区块链”这个概念。

2008 年 10 月 31 日，中本聪发布了《比特币白皮书》。文中，“区块”和“链”这两个字是被分开使用的。

人们用 bitcoin(小写 b)表示比特币,用 Bitcoin(大写 B)表示其底层技术，也就是我们现在说的区块链技术。

2009 年 1 月 3 日，比特币系统开始运行。和前面的区块链原理一样，每一笔银行转账，所有参与的人的电脑都记录一遍，然后相互检查，保证几百万台电脑的账都一模一样，这账就算正式记下了。为了奖励提供电脑来记账的人，每隔几分钟就会在所有记账的电脑中随机奖励一次积分。电脑性能越好，中奖概率就越高。这个记账的过程，就叫做“挖矿”，这个积分，就叫做比特币。这账上记录的就是每个人有多少钱(比特币)。

而支撑比特币体系的主要技术包括哈希函数、分布式账本、区块链、非对称加密、工作量证明,这些技术构成了区块链的最初版本,或称**区块链 1.0 版本**。

直到比特币被广泛使用时，“区块”和“链”才被合称为“区块-链”，到 2016 年才被变成一个词：“区块链”。

由此可见，为何比特币在被众多国家严令禁止的情况下还能够存活这么多年，并且价格越来越高，就是因为它太难被禁了。世界上数十万台记录着同一本比特币账本的计算机，分布在数十个国家的学校机房、普通民宅、深山老林、旷野深处。不管如何打击，只要世界上还有一台机器在跑着比特币账本，它就仍然存在。

然而，比特币等虚拟币为何在很多国家是被禁止交易的呢？

原因是：区块链技术有两面，暗面(不可篡改+匿名)和明面(不可篡改+实名)，目前号称搞区块链技术的，90%以上的虚拟币就是在搞暗面，将不可篡改和匿名这两个属性结合起来，形成了灰色世界中流通的货币。

而社会各方想要扶持的区块链技术，肯定是将不可篡改和实名这两个属性结合起来，形成现实世界中的各种应用。

因此，区块链 1.0 版本之后出现了智能合约，其中定义一些触发条款，条款满足时自动执行合约，扩大了区块链的应用空间，为区块链的快速发展奠定了基础，这就是**区块链 2.0**。

2015 年，《经济学人》杂志发布了封面文章《重塑世界的区块链技术》后，区块链技术在全球掀起一股金融科技狂潮，世界各大金融机构、银行争相研究区块链技术，仅 2016 年就有数十亿美元投资到区块链相关企业当中。

当区块链从货币、金融、市场，开始逐步拓展到政府、健康、科学、文化和艺术等领域后，将进一步改变我们的社会和生活，这就成为**区块链 3.0**。

因此，区块链并不等于虚拟币，后者只是区块链的早期应用。

比特币挖矿机

来源于百度搜索

比特币挖矿机就是用于赚取比特币的计算机。这类计算机一般有专业的挖矿芯片，多采用安装大量显卡的方式工作，耗电量较大。计算机下载挖矿软件然后运行特定算法，与远方服务器通讯后可得到相应比特币，是获取比特币的方式之一[1] 。

比特币挖矿机功能

比特币挖矿机是获取比特币的方式之一。比特币（Bitcoin）是一种由开源的 P2P 软件产生的网络虚拟货币。它不依靠特定货币机构发行，通过特定算法的大量计算产生，比特币经济使用整个 P2P 网络中众多节点构成的分布式数据库来确认并记录所有的交易行为。P2P 的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。

任何一台电脑都能成为挖矿机，只是受益会比较低，可能十年都挖不到一个比特币。很多公司已经开发出专业的比特币挖矿机，这种搭载特制挖矿芯片的

矿机，要比普通的电脑运算速率高几十倍或者几百倍。

比特币挖矿机原理

比特币系统由用户（用户通过密钥控制钱包）、交易（交易都会被广播到整个比特币网络）和矿工（通过竞争计算生成在每个节点达成共识的区块链，区块链是一个分布式的公共权威账簿，包含了比特币网络发生的所有的交易）组成。

比特币矿工通过解决具有一定工作量的工作量证明机制问题，来管理比特币网络—确认交易并且防止双重支付。由于散列运算是不可逆的，查找到匹配要求的随机调整数非常困难，需要一个可以预计总次数的不断试错过程。这时，工作量证明机制就发挥作用了。当一个节点找到了匹配要求的解，那么它就可以向全网广播自己的结果。其他节点就可以接收这个新解出来的数据块，并检验其是否匹配规则。如果其他节点通过计算散列值发现确实满足要求（比特币要求的运算目标），那么该数据块有效，其他的节点就会接受该数据块。

中本聪把通过消耗 CPU 的电力和时间来产生比特币，比喻成金矿消耗资源将黄金注入经济。比特币的挖矿与节点软件主要是透过点对点网络、数字签名、交互式证明系统来进行发起零知识证明与验证交易。每一个网络节点向网络进行广播交易，这些广播出来的交易在经过矿工（在网络上的计算机）验证后，矿工可使用自己的工作证明结果来表达确认，确认后的交易会被打包到数据块中，数据块会串起来形成连续的数据块链。每一个比特币的节点都会收集所有尚未确认的交易，并将其归集到一个数据块中，矿工节点会附加一个随机调整数，并计算前一个数据块的 SHA256 散列运算值。挖矿节点不断重复进行尝试，直到它找到的随机调整数使得产生的散列值低于某个特定的目标。

比特币挖矿机挖矿过程

挖矿是增加比特币货币供应的一个过程。挖矿同时还保护着比特币系统的安全，防止欺诈交易，避免“双重支付”，“双重支付”是指多次花费同一笔比特币。矿工们通过为比特币网络提供算法来换取获得比特币奖励的机会。 矿工们验证每笔新的交易并把它们记录在总帐簿上。每 10 分钟就会有一个新的区块被“挖掘”出来，每个区块里包含着从上一个区块产生到目前这段时间内发生的所有交易，这些交易被依次添加到区块链中。我们把包含在区块内且被添加到区块链上的交易称为“确认”交易，交易经过“确认”之后，新的拥有者才能够花费他在交易中得到的比特币。

矿工们在挖矿过程中会得到两种类型的奖励：创建新区块的新币奖励，以及区块中所含交易的交易费。为了得到这些奖励，矿工们争相完成一种基于加密哈希算法的数学难题，也就是利用比特币挖矿机进行哈希算法的计算，这需要强大的计算能力，计算过程多少，计算结果好坏作为矿工的计算工作量的证明，被称为“工作量证明”。该算法的竞争机制以及获胜者有权在区块链上进行交易记

录的机制，这二者保障了比特币的安全。

矿工们同时也会获取交易费。每笔交易都可能包含一笔交易费，交易费是每笔交易记录的输入和输出的差额。在挖矿过程中成功“挖出”新区块的矿工可以得到该区块中包含的所有交易“小费”。随着挖矿奖励的递减，以及每个区块中包含的交易数量增加，交易费在矿工收益中所占的比重将会逐渐增加。在2140年之后，所有的矿工收益都将由交易费构成。

挖矿是一种将结算去中心化的过程，每个结算对处理的交易进行验证和结算。挖矿保护了比特币系统的安全，并且实现了在没有中心机构的情况下，也能使整个比特币网络达成共识。 挖矿这个发明使比特币变得很特别，这种去中心化的安全机制是点对点的电子货币的基础。铸造新币的奖励和交易费是一种激励机制，它可以调节矿工行为和网络安全，同时又完成了比特币的货币发行。

中本聪

来源：百度搜索

中本聪，自称日裔美国人，日本媒体常译为中本哲史，此人是比特币协议及其相关软件Bitcoin-Qt的创造者，但真实身份未知。中本聪于2008年发表了一篇名为《比特币：一种点对点式的电子现金系统》的论文，描述了一种被他称为“比特币”的电子货币及其算法。2009年，他发布了首个比特币软件，并正式启动了比特币金融系统。2010年，他逐渐淡出并将项目移交给比特币社区的其他成员。中本聪据信持有约一百万个比特币。这些比特币在2013年底时的价值超过十亿美元。

从发表论文以来，中本聪的真实身份长期不为外界所知，维基解密创始人朱利安·阿桑奇（Julian Assange）宣称中本聪是一位密码朋克（Cypherpunk）。另外，有人称“中本聪是一名无政府主义者，他的初衷并不希望数字加密货币被某国政府或中央银行控制，而是希望其成为全球自由流动、不受政府监管和控制的货币。”

2008年11月1日，中本聪在“metzdowd.com”网站的密码学邮件列表中发表了一篇论文，题为《比特币：一种点对点式的电子现金系统》。论文中详细描述了如何创建一套去中心化的电子交易体系，且这种体系不需要创建在交易双方相互信任的基础之上。很快，2009年1月3日，他开发出首个实现了比特币算法的客户端程序并进行了首次“采矿”（mining），获得了第一批的50个比特币。这也标志着比特币金融体系的正式诞生。

2010 年 12 月 5 日，在维基解密泄露美国外交电报事件期间，比特币社区呼吁维基解密接受比特币捐款以打破金融封锁。中本表示坚决反对，认为比特币还在摇篮中，经不起冲突和争议。七天后的 12 月 12 日，他在比特币论坛中发表了最后一篇文章，提及了最新版本软件中的一些小问题，随后不再露面，电子邮件通讯也逐渐终止。

2015 年，加州大学洛杉矶分校金融学教授 Bhagwan Chowdhry 曾提名中本聪为 2016 年诺贝尔奖经济学奖的候选人。

Bhagwan Chowdhry 说：“比特币的发明简直可以说是革命性的。中本聪的贡献不仅将会彻底改变我们对金钱的思考方式，很可能会颠覆央行在货币政策方面所扮演的角色,并且将会破坏如西联这样高成本汇款的服务,彻底消除如 Visa，MasterCard、PayPal 他们收取 2-4%的中间人交易税，消除费事且昂贵的公证和中介服务，事实上它将彻底改变法律合约的方式。”

中本聪极少透露自己的真实信息。在 P2P 基金会网站的个人资料中，他自称是居住在日本的 37 岁男性。然而，这一点被广泛怀疑。他的英文书写如母语般纯熟地道，却从没有使用过日语。用他的姓名在网上搜索，无法找到任何与这个人相关的信息。各种迹象表明，“中本聪”（“中本哲史”）可能是一个虚构身份。中本在发言和程序中切换使用英式英语和美式英语，并且随机在全天不同的时间上线发言，这显示他或者是有意隐瞒自己的国籍和时区，或者是账号的背后有多人操纵。然而，根据对其语言习惯和时间统计的分析，一些人士认为他可能是一位居住在美国中部或西部的英国人或爱尔兰人。曾在比特币核心开发团队工作的 Laszlo Hanyecz 则认为其算法设计过于精良，以至于不像是一个人单枪匹马所能完成。

核稿：张燕　**编辑：**张云春

主送：局领导班子成员，局各处室及直属事业单位。