区块链技术及政策解读

专题研究员

汪颢

☎：（8610）6656 8733

✉：wanghao_yj@chinastock.com.cn

报告完成日期：2019 年 11 月 19 日

报 告 主 要 内 容

●报告主要介绍了区块链技术，及技术特性。

●报告介绍了中共中央政治局第十八次学习提出把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展的精神（以下简称《精神》）出台的背景，重点解读了《精神》与投行相关的内容。

●报告就区块链产业在中国的发展情况作了总结。

●报告详细介绍了区块链技术在行业的落地情况。

目 录

2019 年 10 月 24 日，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。中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要的作用。提出要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

一、背景及意义

区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域。目前，全球主要国家都在加快布局区块链技术发展。我国在区块链领域拥有良好基础，要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展。

（一）各国竞相布局区块链产业制高点

区块链正在被各国认可，并在多领域积极探索技术的推广应用。2018 年 1 月 22 日英国技术发展部门（Innovate UK）相关人士表示，英国将投资 1900 万英镑用于支持区块链等新兴科技领域的新产品或服务。2018 年 2 月 14 日美国众议院召开第二次区块链听证会，“拥抱技术”与“不要封杀”成为共识。韩国央行鼓励区块链技术，韩国唯一的证券交易所 Korea Exchange（KRX）也宣布开发基于区块链技术的交易平台。澳洲在多领域积极探索区块链技术，澳大利亚邮政将区块链技术应用于身份识别。迪拜建立全球区块链委员会，并成立含 Cisco、区块链初创公司、迪拜政府等 30 多名成员的联盟。

（二）区块链技术已具备承载部分垂直行业应用及通用应用开发的能力

从行业发展看，区块链的技术正在走向融合，这使得区块链产业逐渐走向细分。按照区块链产业上下游结构，区块链产业自下而上可以划分为四类：底层基础设施及平台开发、技术扩展及通用型服务、行业应用、产业周边服务。相应的产品归属，可进一步细分为链、客户端、应用等不同类型。继以数字货币为代表的的区块链 1.0 之后，区块链 2.0 所加入的智能合约等相关技术基础已具备承载部分垂直行业应用及通用应用开发的能力。随着区块链革新升级，与云计算、大数据等前沿技术深度融合、集成创新，将促进区块链技术在医疗、司法、工业、媒体、游戏等各个细分领域的商业探索应用。区块链“脱虚向实”趋势明显，行业生态链已初步成形，正在从各个领域助力实体经济高质量发展。

（三）区块链技术能为实体经济与金融市场“赋能”

区块链技术能够广泛服务于支付清算、票据、保险等金融领域以及供应链管理、工业互联网、产品溯源、能源、版权等实体经济领域。几乎所有行业都涉及交易，都需要诚信可靠的交易环境作为行业健康发展的前提支撑。区块链技术通过数学原理而非第三方中介来创造信任，可以降低系统的维护成本。对于传统金融机构而言，对账、清算、审计等线上环节的运营与人力成本将得以降低；对于非金融行业，区块链能够减少价值链各环节的信息不对称，从而提升协作效率，降低整体交易成本；对于个体而言，陌生双方或多方能够跨越物理距离的限制，在网络上安全传递价值，从而创造更多供给与需求。

二、主要内容总结

为把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展，中共中央总书记习近平提出了以下几点要求：

（一）要强化区块链的理论基础研究，一方面提升国际话语权和规则制定权，另一方面构建区块链产业生态。

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。要推动协同攻关，加快推进核心技术突破，为区块链应用发展提供安全可控的技术支撑。要加强区块链标准化研究，提升国际话语权和规则制定权。要加快产业发展，发挥好市场优势，进一步打通创新链、应用链、价值链。要构建区块链产业生态，加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合，推动集成创新和融合应用。要加强人才队伍建设，建立完善人才培养体系，打造多种形式的高层次人才培养平台，培育一批领军人物和高水平创新团队。

（二）要推动区块链和实体经济深度融合，尤其强调运用区块链解决中小企业贷款融资难、银行风控难、部门监管难等问题。

要抓住区块链技术融合、功能拓展、产业细分的契机，发挥区块链在促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系等方面的作用。要推动区块链和实体经济深度融合，解决中小企业贷款融资难、银行风控难、部门监管难等问题。要利用区块链技术探索数字经

济模式创新，为打造便捷高效、公平竞争、稳定透明的营商环境提供动力，为推进供给侧结构性改革、实现各行业供需有效对接提供服务，为加快新旧动能接续转换、推动经济高质量发展提供支撑。要探索“区块链+”在民生领域的运用，积极推动区块链技术在教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用，为人民群众提供更加智能、更加便捷、更加优质的公共服务。要推动区块链底层技术服务和新型智慧城市建设相结合，探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理的智能化、精准化水平。要利用区块链技术促进城市间在信息、资金、人才、征信等方面更大规模的互联互通，保障生产要素在区域内有序高效流动。要探索利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，深化“最多跑一次”改革，为人民群众带来更好的政务服务体验。

（三）要加强对区块链安全风险的研究和分析，推动区块链安全有序发展。

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，密切跟踪发展动态，积极探索发展规律。要探索建立适应区块链技术机制的安全保障体系，引导和推动区块链开发者、平台运营者加强行业自律、落实安全责任。要把依法治网落实到区块链管理中，推动区块链安全有序发展。

相关部门及其负责领导同志要注意区块链技术发展现状和趋势，提高运用和管理区块链技术能力，使区块链技术在建设网络强国、发展数字经济、助力经济社会发展等方面发挥更大作用。

精神解读

在一系列的政策扶持下，区块链技术在我国迅速发展并与各行各业深度融合。如今，以创造社会价值、赋能实体经济为核心已成为大势所趋。对于区块链的认识，我们也要与时俱进：既要讲当前，更要讲长远；既要看国内，更要看全球；既要防风险，更要促发展，特别对于其在建设网络强国、发展数字经济、助力经济社会发展等方面的巨大作用更要有深刻、系统、完整的认识。

第一，我国对区块链的战略定位高。要用发展的眼光看区块链技术，不能低估它的明天。必须落实总书记部署，把区块链作为核心技术自主创新的重要突破口。本次学习强调要努力让我国在区块链这个新兴领域走在理论最前线、占据创新制高点、取得产业新优势。

第二，要用科学的眼光看区块链标签，不能高估它的今天。我国在区块链领域拥有良好基础，

要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展。预计在政策红利及产业资本助力下，我国区块链技术应用有望快速发展。

第三，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用，要继续用战略的眼光看区块链产业。关注后续区块链与 5G、人工智能、物联网等技术的不断融合和落地应用。

三、我们对于区块链的认识

（一）区块链的概念

区块链（Blockchain）是一种由多方共同维护，使用密码学保障传输和访问安全，能够实现数据一致储存、难以篡改、防止抵赖的记账技术，也称为分布式账本技术（Distributed Ledger Technology）。典型的区块链以块-链结构存储数据。作为一种在不可信的竞争环境中低成本建立信任的新型计算范式和协作模式，区块链凭借其独有的信任建立机制，正在改变诸多行业的应用场景和运行规则，是未来发展数字经济、构建新型信任体系不可或缺的技术之一。

（二）区块链的特征

相对于传统的分布式数据库，区块链体现了以下几个对比特征：

1. 从复式记账演进到分布式记账

传统的信息系统，每位会计各自记录，每次对账时存在多个不同账本。区块链打破了原有的复式记账，变成“全网共享”的分布式账本，参与记账的各方之间通过同步协调机制，保证数据的防篡改和一致性，规避了复杂的对方对账过程。

2. 从“增删改查”变为仅“增查”两个操作

传统的数据库具有增加、删除、修改和查询四个经典操作。对于全网账本而言，区块链技术相当于放弃了删除和修改两个选项，只留下增加和查询两个操作，通过区块和链表这样的“块链式”结构，加上相应的时间戳进行凭证固化，形成环环相扣、难以篡改的可信数据集合。

3. 从单方维护变成多方维护

针对各个主体而言，传统的数据库是一种单方维护的信心系统，不论是分布式架构，还是集中式架构，都对数据记录具有高度控制权。区块链引入了分布式账本，是一种多方共同维护、不存在单点故障的分布式信息系统，数据的写入和同步不仅仅局限在一个主体范围之内，需要通过多方验

证数据、形成共识，在决定哪些数据可以写入。

4. 从外挂合约发展为内置合约

传统上，财务的资金流和商务的信息流是两个截然不同的业务流程，商务合作签订的合约，在人工审核、鉴定成果后，再通知财务进行打款，形成相应的资金流。智能合约的出现，基于事先约定的规则，通过代码运行来独立执行、协同写入，通过算法代码形成了一种将信息流和资金流整合到一起的“内置合约”。

（三）区块链的关键机制：

1. 密码学原理

① 哈希算法

哈希算法是一类加密算法的统称，是信息领域中非常基础也非常重要的技术。输入任意长度的字符串，哈希算法可以产生固定大小的算出。

② 非对称加密

非对称加密是指加密和解密使用不同秘钥的加密算法，也称公私钥加密。使用这个密钥对时，如果用其中一个密钥加密一段数据，则必须用另一个密钥解密。

2. 数据存储结构：默克尔树

默克尔树（Merkle Tree）实际上是一种数据结构。这种数据结构在快速归纳和检验大规模数据完整性方面效率很高。在比特币网络中，默克尔树被用来归纳一个区块中的所有交易，其树根就是就是整个交易集合的哈希值，只要记住根节点哈希，树中的任一个节点被篡改，根节点哈希就不会匹配，从而达到校验目的。

3. 共识机制

共识机制是区块链网络最核心的秘密。简单来说，共识机制是区块链节点就区块信息达成全网一致共识的机制，可以保证最新区块链被准确添加至区块链、节点存储的区块链信息一致不分叉甚至可以抵御恶意攻击。

（四）区块链两大核心性质

1. 分布式记账与存储

在记账方面，区块链不需要依赖一个中心机构来负责记账，而是通过“全网见证”，所有交易

信息会被“如实地记录”，而且这个账本是唯一的。

在存储方面，由于网络中的每一个节点都有一份区块链的完整副本，即使部分节点被攻击或者出错，也不会影响整个网络的正常运转。同时由于每个节点都有一份副本也意味着所有的账目和信息都是公开透明、可以追溯的。

2. 不可篡改

在区块链中伪造、篡改账目基本是不可能的，不可篡改也意味着数据的高度一致和安全性。

区块链中的交易无法被伪造的原因在于，首先，合法的交易需要私钥签名，否则无法被其他节点验证；其次，每一笔交易都是可回溯的，也就杜绝可无中生有的可能。

（五）区块链技术的应用

根据实现方式和作用目的的不同，当前基于区块链技术的应用可以化为为三类场景，如下表所示：一是价值转移类，数字资产在不同账户之间转移，如跨境支付；二是存证类，将信息记录到区块链上，但无资产转移，如电子合同；三是授权管理类，利用智能合约控制数据访问，如数据共享。此外，随着应用需求的不断升级，还存在多类型融合的场景。

表 1 区块链应用场景分类

类型	政府	金融	工业	医疗	法律	版权
价值转移		数字票据 跨境支付 应收账款 供应链金融	能源交易	医疗保险		
存证	电子发票 电子证照 精准扶贫	现钞冠字号溯源 供应链金融	防伪溯源	电子病历 药品追溯	公证 电子存证 网络仲裁	版权 确权
授权管理	政府数据 共享	征信		健康数据 共享		版权 管理

（六）前景展望：技术融合、智能合约将是未来趋势

区块链作为对传统信息技术的升级与补充，其发展将与其他新兴信息技术相互融合、相互促进。当前区块链仍处于发展发展初期，不仅需要政府、行业联盟、企业合作技术标准和共识机制，更离不开 5G、物联网、人工智能、大数据等技术的支持。

1. 技术融合

① 5G。大型公链的每秒交易量有限、交易确认时间长。未来 5G 网络大范围商业化应用后可大

幅提升书记传输速度、减少网络拥堵，大型公链的性能将得以提升并逐渐适用于每秒上万笔交易的商业应用场景。

② 物联网。当前区块链技术仅能解决链上的信任问题，但对于链下数据的真实性与准确性几乎无能为力。物联网技术进一步发展后，链下数据的观测、采集、处理、更新都将实现自动化，真实性和准确性得到有力保证，区块链的应用场景也将得到扩展。

③ 人工智能。工作量证明机制被诟病浪费了大量电力与硬件资源，目前比特大陆等矿机生产商已经和比原链合作开发应用于人工智能算法的共识机制与芯片，将哈希计算转化为应用于深度学习的矩阵计算，创造更大的经济与社会价值。

2. 智能合约

智能合约可能是区块链上最具革命性的应用。如果智能合约在区块链上实现广泛运用，经济分工将在互联网时代进一步细化，更广泛的社会协同将得以实现。通过智能合约的广泛运用，区块链将创造多个特定领域的线上细分市场，直接对接全球范围内各网络节点的需求和生产。网络拓扑意义上的分工协同与地理意义上的分工协作将形成更紧密和更深层次的互补，区块链也有望从“信任机器”升级成产业浪潮的重要“引擎”。

四、区块链技术详解

1. 非对称加密技术

区块链技术中主要应用非对称加密技术。保密的原理如下，在网络中传输的数据并不是明文，而是经过加密的暗文，只有用密钥才能解密转化为可读明文。如果没有密钥，即使网络上其他用户截获了你的信息，也无从阅读理解，从而保证了信息传递的保密性。传统的对称加密，由于加密和解密是可逆的，对称加密的速度快，它的加密和解密的密钥是同一把，而非对称加密中加密和解密是用不同的密钥，其中公开的密钥称之为公钥，个人保存的密钥称之为私钥。如果用公钥加密，那么就必须用私钥解密，如果用私钥加密，就必须用公钥解密。而对称加密在密钥保存方面存在缺陷，对称加密好比在一个公共的安全箱里面放了一封信，安全箱通过同样的钥匙打开，寄信人和收信人必须每人保留一把一模一样的钥匙。两个陌生人通信前要首先传递密钥，然后才能进行通讯。

但是密钥本质上也是一个数据，它的传递也需要一个安全箱作为载体来保证安全。没有密钥就没有安全箱，没有安全箱难以安全的传递密钥，一旦密钥传递过程中被窃取，那么通信的安全并不能得到保证。而非对称加密可以解决这个问题，非对称加密的安全箱特殊设计成两端开口的管型，每个口各自有一把钥匙，信件在管道里面只能单向运动不能回头。对外的管道口用公钥才能打开，公钥是公开的，意味着每个人都可以通过管道给你发送信息传递数据。但是只有拥有私钥的你可以打开另一端的管道口阅读，别人是无从知晓的。当用户要给别人发送信息时，只需要找到对方的公钥，打开管道口，将信息和数据传进去，对方变可在另一边用私钥解密查看了。同对称加密比，非对称加密和解密速度慢。

2.散列函数生成“数字指纹”保证数据一致

散列函数的主要功能就是对每一段数据生成其独一无二的“数字指纹”，在互联网中被频繁的传递，保证接受数据同发送数据完全一致是极其重要的，这就是需要找到数据的“数字指纹”来确定它。无论是什么类型的数据（图像、字符、程序），其底层都是 0、1 二进制数字串，科学家发明了一种散列函数（Hash 哈希函数），可以将输入的任意长度的数据缩短为一个固定长度的字母数字组合字符串，称之为 Hash 值，它是输入数据的摘要（“数字指纹”），它具备以下的特征：1. 单向求解：你可以通过指纹确认一个人身份，但是指纹无法告知他的长相等详细信息。同理，每个数据都有唯一的 Hash 值（“数字指纹”），通过源数据计算 Hash 值十分快，方向通过 Hash 值无法反推出数据全文。2.强确定性，散列函数是一类函数的统称，如果用具体的某个散列函数（例如比特币区块中使用 SHA256 函数）对输入数据求解 Hash 值，一样的 Hash 值几乎一定对应完全一样的输入数据。这里用的是几乎一定而不是完全一定，因为在极小的概率下，可以通过计算机穷举算出一个数据同伪造对象数据得出的一样的 Hash 值，这样的计算叫做碰撞攻击。3. 强混淆性：输入一些数据计算出 Hash 值，然后部分改变输入值，会产生一个完全不同的 Hash 值，即便改变一个标点符号都会得到一个完全不一样的哈希值。

数字指纹 Hash 值在实际场景中常用来校验数据防篡改。例如，发送方会公布发送数据的 Hash 值，接收方接受数据之后也计算数据的 Hash 值，二者如果完全一致，则可认为接收的数据和发送的数据完全一致未经篡改。

3.数字签名证明数字真实性

真实性是两个层面的：发送内容真实，发送者身份真实。Hash 值的比较可以得出数据真实性判断，还需要配合非对称加密技术来确认数据发送者身份的真实，这就是“数字签名”的作用。发送者首先用散列函数求出发送数据的 Hash 值（“数字指纹”），然后用自己的私钥对其进行加密，加密后生成一个暗文的字符串，这就是数字签名，发送信息的时候将这一段数字签名附加在其后，接受数据方首先对签名进行公钥解密，只有用发送者的公钥才可以解开，以此完成了发送者身份确认。同时对数据求解散列值，同解密后的散列值进行对比，如果二者相同，就证明数据是真实未篡改的。

4. 如何记账——共识机制（记账权分配）

一笔又一笔的交易以交易单形式向全网广播，网络上每个节点都在接收全网的所有交易单，把它们放在本地一个临时的账单（区块）当中。所有用户都参与维护账单，就出现以谁的账单为准的问题，每个节点在网时间不同，网络传输状况不同，接收到的交易单也可能不同，如何分辨对错就是记账权分配问题。目前有三种记账权分配机制：POW（Proof of work，工作量证明），POS（Proof of Stake，权益证明），DPOS（Delegate proof of Stake，股份授权证明机制）等，比特币中采用的是 POW，越来越多的其他数字货币采取了 POS 和 DPOS，或者是几种机制的混合。

4.1 POW 工作量证明：计算能力的比拼

工作量证明机制隐含的逻辑是，努力工作的会计应该大概率是诚实可信的。一个会计（比特币中称为矿工）为了获得通过工作量证明获得记账权需要进行一 下的步骤：

1.收听全网的广播，比对本地账本筛查拒绝掉一些不合理的交易单（例如余额不足的），将合理的新交易单记录在本地账单之中。

2.计算一个随机数 X，将 X 同本地账本衔接一起计算一个 Hash 值。

3.Hash 值需要前面若干位是 0（位数调整影响计算难度），而这样的随机数很难算出，需要进行上亿次的计算（挖矿过程）。

4.一旦计算出来之后满足要求的随机数，即刻向全网广播，全网的其他节点用他们本地的账单+随机数进行 Hash 值计算验证，验证通过之后就以该节点的账单为准进行对账。记账节点获得货币奖励。

5.对账完成，进行新的一轮随机数计算竞赛（挖矿竞赛），争夺记账权。比拼核心：计算能力（不停的穷举随机数）。

4.2 POS 权益证明：权益大小的比拼

权益证明机制隐含逻辑是：区块链应该由那些在其中有经济利益的人进行保障，持有大量数字货币的节点更希望交易是真实可信的，保证数字货币的公信力以此保护自己的利益。介绍 POS 之前需要介绍“币龄”（或者称为钱币权益）。币龄简单来说，就是一个根据你持有货币的量和时间，给你发利息的一个制度，在股权证明 POS 模式下，每个币每天产生币龄，比如你持有 100 个币，总共持有了 30 天，那么，此时你的币龄就为 3000，这个时候，如果你发现了一个 POS 区块，你的币龄就会被清空为 0。你每被清空 365 币龄，你将会从区块中获得 0.05 个币的利息(可理解为年利率 5%)，那么在这个案例中，利息=3000 *5%/365=0.41 个币，持币有利息。权益证明的运行过程如下：

1.收听全网的广播，比对本地账本筛查拒绝掉一些不合理的交易单（例如余额不足的），将合理的新交易单记录在本地账单之中。

2.构造一笔自己向自己支付的交易，将本地账单同含有币龄数据的自交易单衔接，计算得到一个 Hash 值，这个计算每隔秒进行一次（币龄会更新）。

3.Hash 值需要满足 POS 机制的要求，这样也就使得计算难度同币龄成反比，币龄增长相当于过去的穷举随机数。

4.一旦计算出来满足要求的 Hash 值，即刻向全网广播，其他节点进行 Hash 值计算验证，验证通过之后就以该节点的账单为准进行对账。记账节点清空支出的币龄（货币回到账户，只是持币时间归零，相当于币龄清空）

5.对账完成，进行新的一轮计算，争夺记账权。

比拼核心：愿意支付的币龄（自己给自己转账的金额）

4.3 DPOS 股份授权证明机制：电子民主

DPOS 是网络时代的电子民主制度，完全不同于 POW 和 POS 随机选取的共识，是基于信任产生的代议制。首先选取全网 101 个受托人，他们按照顺序对特定时间段进行记账，他们之间采取直连保证通讯安全。

比拼核心：节点信任，成为受托人。

5.如何成链——共识机制（侧链消除）

区块排列：传统账单的页码是连续的数字，而区块链账单的页码是前十位数字为 0 的超长随机数密码（Hash 哈希算法生成）。在区块链账单中，需要指定上 一页的页码，才能将区块有序排列。每一个区块是使用密码学签名与下一个区块'链接'起来的。区块头中的"本区块哈希值"相当于账单的"本页页码"，"父区块哈希值"相当于"上页页码"。而"页码"的具体数值是使用上一页"正文"的全文作为自变量，通过哈希函数生成的随机字符串。网络里的计算机要争夺记账权，就必须随机生成到前十位数字是 0 的"页码"，而随机数的前十位为 0 是个极端罕见的事件，因此整个区块链网络也需要花 10 分钟左右的时间，才可能由某台计算机找到一个这样的"页码"。一旦找到，这台计算机就夺得了记账权，它所生成的新账单（一个账单 4000 笔交易，平均一秒钟 7 笔）（区块）就会更新到网络中的所有计算机。账单（区块）通过上页页码（父哈希）寻找父区块，自动链接成为账本（区块链）。

区块链的不可篡改性由共识机制保证。最长的链条才被全网公认。如果某个人想要篡改数据，链条就会出现分支。为了让别人认可这条伪造的链条，他必须以个人力量维持这支链条直到其长度大于真正的链条。由于工作量证明机制，记录每个区块都需要耗费大量的算力；而且单个节点的算力必须超过全网 51%的算力才有可能超过真正的链条长度。随着系统的壮大，这一点几乎不可能实现。

五、区块链发展现状

（一）全球区块链发展现状

1. 监管体系逐渐完善

欧美高度重视区块链产业与监管并行发展：一是美国程度坚持产业与监管双管齐下。二是欧盟各国高速重视区块链体系的建设。

日韩等亚洲国家力图通过区块链抢占新兴技术制高点。日本积极探索区块链发展道路，并从发展中探索监管之路，目的是全球区域链领域弯道超车，发挥关键作用。韩国鼓励探索区块链技术，

全面铺开区块链金融服务试点，争夺亚洲金融科技中心。阿联酋积极研究区块链技术，迪拜和阿布扎比开展了多个支持技术创新和创意养成的项目。印度依托其成熟的软件产业，积极与亚洲国家开展区块链合作研究。泰国区块链技术在东盟地区处于领先地位，泰国相关监管部门表示将做出相应调整来积极支持区块链技术发展，应对市场变化。

2. 标准制定初现成效

区块链作为一种颠覆性的创新应用模式，其广泛的应用在创造价值的同时也带来了挑战，尤其是现阶段各行业缺乏核心的理念和基本技术共识，使得行业发展碎片化。因此，相关标准的制定对于全球区块链技术发展具有重要意义。在密码算法和签名标准方面，国际标准密码算法已经较为成熟，代表算法分别有 DES、AES、RSA、SHA 系列等。

在区块链技术标准方面，国内外标准化组织在近两年纷纷加快了区块链标准化工作，在标准化前期研究、组织建设和标准研制等方面取得了一些进展。

3. 核心架构趋于成熟

随着区块链技术在不断的升级与迭代，核心架构也已趋于成熟。实际上，区块链并没有特殊创新的技术，而是跨领域将过去数十年包括计算机科学、密码学、分布式系统、P2P 网络等学科理论和技术进行创新整合的成果。可以看到，当前基本形成了以密码学、分布式系统、P2P 网络为主，多种改良技术为辅的区块链技术体系。随着区块链技术创新发展，区块链技术体系会愈发完善。

4. 产业规模持续增长

赛迪区块链研究院根据 Gartner、QYResearch、Tractica 等调研机构的公开数据进行整理，2016 年全球区块链市场规模为 2.28 亿美元，市场进入活跃期，融投资事件不断增多，2017 年全球区块链直接市场价值达到 4.1 亿美元，同比增长 79.8%。随着各国对区块链技术的逐渐重视，对加密数字货币的监管逐渐完善，区块链技术架构也趋于成熟，2018 年全球区块链市场规模迎来爆发，达到 46 亿美元左右，复合增长率达到 172.23%。。赛迪区块链研究院整理国际数据公司 IDC 报告公开数据，2018 年全球区块链解决方案市场规模达到 21 亿美元，其中，美国将占到全球区块链支出的 40%，西欧将成为第二大地区，中国位列第三。

5. 行业应用不断拓展

金融行业率先应用区块链技术并逐渐区域成熟；医疗行业成为区块链应用的重要领域；溯源存

证服务需求迅速攀升；区块链 BaaS 服务平台逐渐发力；随着智能制造与物联网的快速崛起，区块链与制造业及物联感知领域的结合也成为必然趋势。此外，全球各国在零售、房地产、社会公益、旅游、物流等多个领域均开始探索区块链应用场景。

（二）我国区块链发展总体现状

1. 政策驱动与监管加速产业发展

一是国家出台相关政策超前布局区块链发展，积极推动区块链与大数据、人工智能、云计算等信息化技术的融合，鼓励区块链技术在金融科技等领域的创新应用。

二是地方政府从基础设施建设、产业扶持、技术研发创新以及产业应用落地等角度积极出台配套政策支持区块链产业发展。2016 年至今，北京、上海、深圳、广州等各大城市纷纷出台区块链相关政策，贯彻国家有关区块链发展战略，积极鼓励、支持区块链产业发展，推动区块链应用落地。全国 29 个已经出台区块链相关政策的省级行政区，共 149 条区块链相关政策规划。

三是国家及地方监管部门不断探索区块链监管体系的建设，及时出台规范措施，优化区块链产业环境，坚决遏制假借区块链技术的非法金融活动。

2. 行业标准与规范制定继续完善

自 2016 年起，我国区块链标准制定进入起步阶段，并在 2018 年取得一定进展。2018 年我国区块链标准及行业规范制定相关重要会议和事件达到 10 次以上。同时，我国积极参与国际组织区块链标准制定工作，在 ISO/TC 307《区块链及电子化的分布式账本技术》标准制定中承担分类和本体的编辑以及参考架构的联合编辑职务。

3. 核心技术与创新能力不断提升

一是区块链技术研究得到重视，研究团队不断增多。根据赛迪区块链研究院整理，我国目前区块链研究机构数量为 68 家，其中北京、杭州、上海、深圳、贵阳等地区块链研究机构较多。

二是国内企业及研究团队在区块链技术方面取得重要成果。40 家区块链重点企业核心技术一览表见附件二。

三是专利申请走在世界前列。根据赛迪区块链研究院与链塔智库数据显示，2018 年中国在区块链专利申请数量上领先全球，专利数量约占到世界主要国家区块链专利数量的 67%。

4. 产业规模与竞争实力持续升级

截至 2018 年 12 月，我国提供区块链专业技术支持、产品、解决方案等服务，且有投入或产出的区块链企业共 672 家，区块链产业规模约 10 亿元，区块链相关产品交易、教育等衍生产业的规模约为 40 亿元。

5. 行业应用于平台服务加速推进

在区块链企业、互联网企业、应用企业、第三方服务机构等多方的共同推进下，我国区块链应用正持续展开。一批新产品、新平台、新服务不断涌现，以合作共建、平台先行为突出特点的应用模式持续显现。但整体上来看，当前我国区块链行业应用仍处在起步阶段，形成的应用产品有待市场验证，建设的应用平台还需实际落地。

（三）我国区块链产业发展现状

2018 年以来，我国区块链产业进入快速发展阶段，总体而言，我国区块链产业发展仍处于初级阶段，但市场规模潜力巨大。

1. 产业链条基本形成，产业规模快速增长

区块链的产业链上游主要包括硬件基础设施和底层技术平台层，该层包括矿机、芯片等硬件企业，以及基础协议、底层基础平台等企业；中游企业聚焦于区块链通用应用及技术扩展平台，包括智能合约、快速计算、信息安全、数据服务、分布式存储等企业；下游企业聚焦于服务最终的用户(个人、企业、政府)，根据最终用户的需要定制各种不同种类的区块链行业应用，主要面向金融、供应链管理、医疗、能源等领域。

我国从事提供区块链产业底层技术平台服务、应用产品、行业技术解决方案服务等业务,具有投入产出的区块链企业共 672 家，主要聚集在北京、上海、广东、浙江、四川、江苏等地。其中北京最多，区块链企业数量为 219 家，约占全国 32.59%；上海排名第二，共有区块链企业 162 家，约占全国 24.11%；广东排名第三，共有区块链企业 144 家企业，约占全国 21.43%；北京、上海、广东、浙江、四川、江苏等地共有区块链企业 609 家，约占全国区块链企业总数的九成。

表 2 我国区块链企业各地区分布数量及比例

地域	数量（家）	比例	地域	数量（家）	比例
北京	219	32.59%	河北	2	0.27%

上海	162	24.11%	河南	2	0.27%
广东	144	21.43%	江西	2	0.27%
浙江	51	7.59%	辽宁	2	0.27%
四川	20	2.98%	黑龙江	1	0.14%
江苏	13	1.78%	吉林	1	0.14%
福建	9	1.23%	甘肃	1	0.14%
重庆	7	0.96%	广西	1	0.14%
山东	6	0.96%	云南	1	0.14%
陕西	5	0.68%	内蒙古	1	0.14%
贵州	5	0.68%	宁夏	1	0.14%
安徽	3	0.41%	山西	1	0.14%
湖北	3	0.41%	青海	0	0.00%
湖南	3	0.41%	新疆	0	0.00%
天津	3	0.41%	西藏	0	0.00%
海南	3	0.41%	总计	672	100%

我国区块链产业应用领域分布情况如图 1 所示，我国区块链产业应用主要分布在金融、供应链、溯源、硬件、公益慈善、医疗健康、文化娱乐、社会管理、版权保护、教育和共享经济等领域。其中从事“区块链+金融”领域的企业有 179 家，占 26.6%；金融、供应链、溯源、硬件、公益慈善四个领域领跑区块链应用，共有区块链企业 401 家，约占总数的 60%。2018 年以来，我国区块链相关应用日益趋向多样化，区块链技术在医疗健康、文化娱乐、社会管理、版权保护、教育和共享经济等领域增长趋势明显。

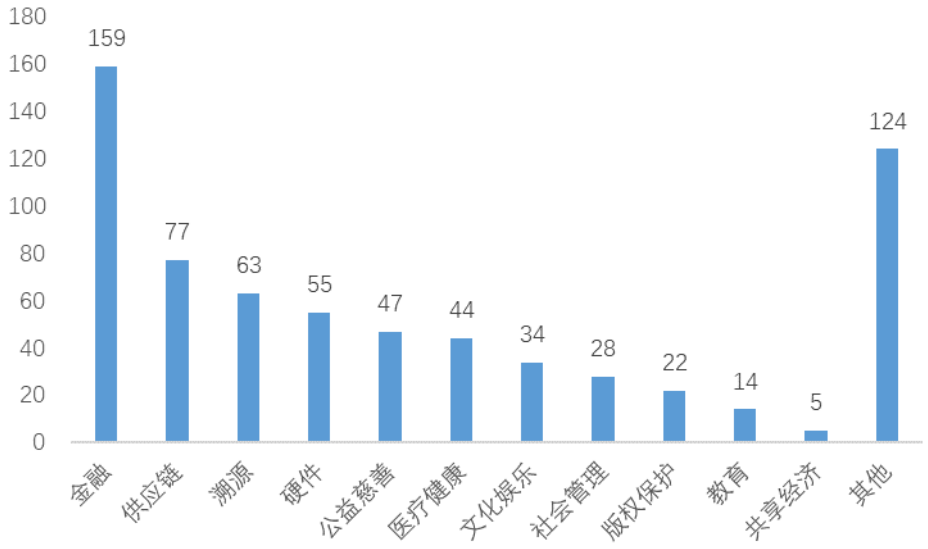

图 1 我国区块链应用分布领域

2. 初创企业实力渐显，巨头企业强势加入

根据赛迪区块链研究发布的区块链初创企业百强榜单，包括云象、阿尔山、天德科技、太一云、数秦科技等区块链初创企业纷纷入选。各企业的团队实力、科研实力、创新实力、产品竞争力以及运营能力均表现优异，企业研发团队占比超过五成的企业达到 73 家，实现企业盈利的企业占比接近 70%。

随着区块链技术得到广泛认可，产业应用潜力逐渐显现，各大银行、科技巨头也纷纷强势加入，据赛迪区块链研究院统计，目前正在进行区块链应用探索的国内银行机构共 34 家，其中包括了人民银行、四大国有商业银行、各地区城市银行、股份制商业银行以及民营银行。

3. 技术研发技术扎实，核心技术创新升级

专利方面，目前我国已成为国际区块链专利高产国家，一批具有较高价值度的区块链专利不断涌现。此外，科技及互联网巨头也在区块链技术研发中取得重要突破，其中阿里巴巴集团、中国平安、复杂美等企业在 2019 年上半年公开的区块链专利数量方面均超过 100 项，在全球区块链发明专利申请数量前二十的企业中，中国公司占据 15 席。2019 年上半年公开的全球区块链发明专利申请数量，如下表所示。

表 3 我国企业区块链相关专利申请及累计情况

排名	公司名称	2019 年上半年公开	国别/地区

		的全球区块链发明专利申请数量/件	
1	阿里巴巴集团控股有限公司	322	中国
2	中国平安	274	中国
3	Nchain	241	安提瓜和巴布达
4	复杂美	122	中国
5	IBM	104	美国
6	众安科技	99	中国
7	百度	90	中国
8	元征科技	86	中国
9	中国联通	81	中国
10	MasterCard	79	美国
11	网新科技	74	中国
12	趣链科技	66	中国
13	腾讯	66	中国
14	京东	59	中国
15	Siemens	55	德国
16	中链科技	52	中国
17	点融	51	中国

18	**金链通**	46	**中国**
19	**泰康**	41	**中国**
20	Accenture	37	**爱尔兰**

4. 企业资金运作良好，金融资本持续涌入

投融资方面，2017 年至 2018 年，我国区块链领域投融资频次和金额急剧增加，多个区块链企业和项目获得大额投资。2016 年相较于 2015 年有飞跃式增长，融资额约 11 亿元，年增长率约 1367%；2017 全年区块链领域融资额约 19 亿元，较 2016 年增长约 73%。2018 年全年，区块链领域投融资保持高速增长，融资额约 154.9 亿，同比增长达 715%。截至 2018 年 12 月，涉及区块链相关主题的投融资事件达 384 件，同比 2017 年增长 241%，中国区块链行业投资热度上升明显。

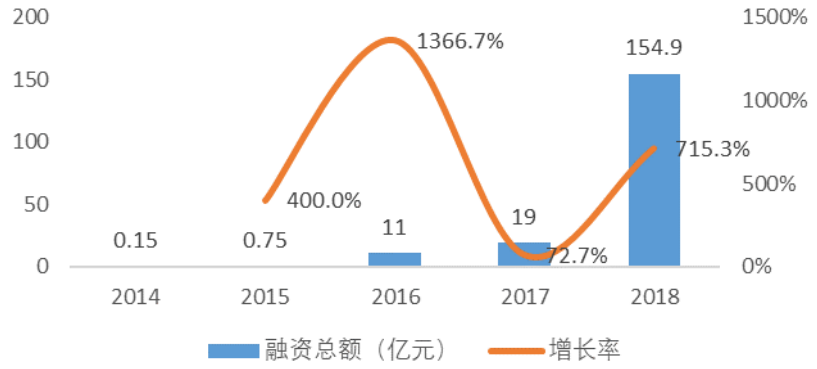

图 2 我国区块链领域年度投融资总额及增长率

从融资轮次分布来看，获得 Pre-A/A 轮和天使轮/种子轮投资的企业最多，分别达 33 家和 28 家。符合区块链行业处于早期发展阶段的特征。从融资金额分布来看，在已知获得融资的百强企业中，42%的企业融资金额在 1000 万至 5000 万人民币之间。其次是融资金额在 1000 万人民币以下的企业，占 32%。

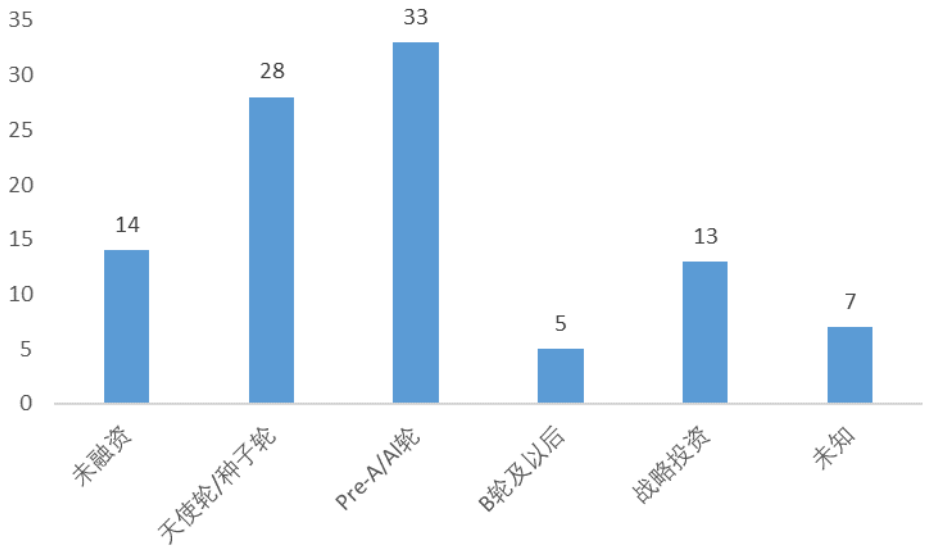

图 3 区块链企业融资轮次分布（数据来自赛迪研究院）

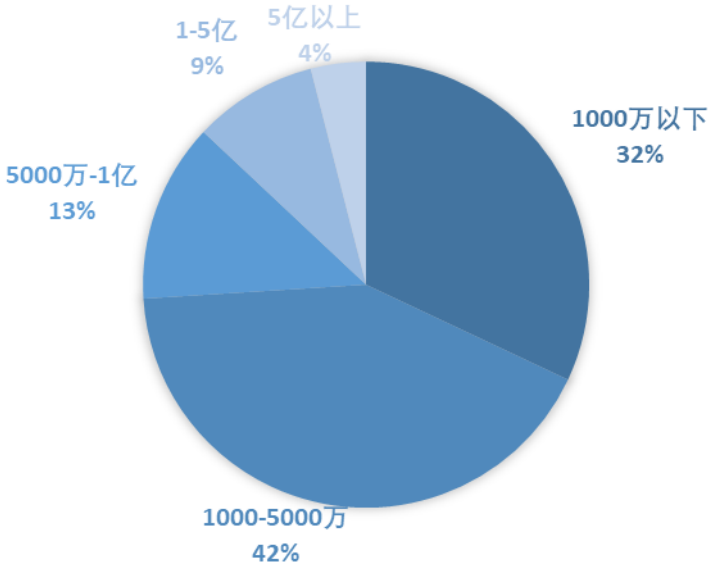

图 4 区块链百强企业融资金额分布（数据来自赛迪研究院）

5. 区域优势影响显著，政策驱动效果渐显示

根据赛迪区块链研究院发布的《2018 年发布的中国城市区块链发展水平评估报告》结果显示，传统 4 座一线城市北上深广分别处于第一、三、四、六名。杭州作为近年在互联网产业发展迅速崛起的城市代表，依靠长江三角洲发达经济优势和产业基础，在新兴技术产业发展方面继续保持良好势头，取得评估结果的第二名。总的来看，长江三角洲地区和珠三角地区等发达地区城市具有明显的经济和科技等先天优势，引领全国区块链产业发展。

6. 聚集要素逐渐积累，产业园区不断涌现

区块链产业园区作为区块链产业集群发展的重要载体，各地方政府正在加快推进建设。截止到2018 年 12 月，我国已经成立或者在建区块链产业园区的城市约 20 余个。其中，除海口区块链产业园、中国（萧山）区块链创业创新基地两个产业园是由企业出资发起外，其余园区均为当地政府主导成立的，并配有相关入驻政策扶持。

（四）我国区块链行业应用现状

我国企业在区块链技术应用方面正处在积极探索阶段，呈现出两个主要特点。一是大型行业企业积极应用区块链技术来改进其自身的业务，但仍以尝试为主，主要的应用场景也都为行业中的非核心业务。如中国平安、中国银联、蚂蚁金服等企业在区块链应用探索中仅限于非核心业务。二是以区块链技术服务为主的企业的业务发展大多处在起步阶段，产品技术体系和商业模式还不够成熟，需求方对区块链的认识还有待提高。

1. 金融应用全面开展

目前为止，金融领域是区块链技术介入最多，也是需求最大的一个领域。。据不完全统计，包括国有四大银行和主要股份制银行在内的国内大型银行均已布局区块链，主要涉及供应链金融、资产托管、跨境清算、公益捐款、联合放贷等方面的应用。

2. 医疗领域刚刚起步

区块链技术中密码学算法能在去中心化的环境中更好保护病人的隐私，大幅度改善医疗质量和医疗管理模式，降低医疗成本和风险，医疗领域出现了对区块链技术的强烈需求并面临广阔的应用前景。未来医疗行业区块链应用将沿两个方向发展：一是区块链企业和地方政府合作推动基于区块链的医疗行业服务平台建设；二是区块链企业与医院联合建设基于区块链的医院综合管理信息系统。

3. 溯源存证效果显著

区块链在电子存证领域的主要应用是利用区块链技术的时间戳、不可篡改等功能实现数据真实性证明。截止 2018 年 12 月，在电子存证区块链联盟“法链”的推动下，我国电子存证领域区块链应用快速发展，在多个细分领域涌现出了一批应用案例。

4. 慈善应用步步为营

公信力是慈善机构的生命线，其地位不言而喻。区块链技术有望成为解决慈善机构公信力的重要法宝。当前，在慈善领域，区块链基础产品研发取得一定突破，互联网企业基于区块链的慈善平台已经上线，区块链应用正在逐步展开，并不断取得进步。

5. 政务服务快速启动

政府数据的开放共享是推进大数据发展的重要组成部分，区块链技术应用在政务领域，将有助于政府数据的共享开放。但由于我国各地政府信息化发展水平不一，对区块链等新兴信息技术的应用理解有限，政务服务应用步伐相对较慢。一些信息化推进较快地区开始尝试利用区块链技术服务于政务领域，佛山、贵阳等地在积极探索开展区块链政府服务应用。

6. 物流应用有待突破

针对物流领域环节长、角色多、流程复杂等行业痛点，基于区块链技术共识机制和分布式存储机制，通过将所有物流参与者的数据连接并记录到区块链网络中，有效解决因物流参与方信任未知和物流信息离散而产生的物流纠纷问题，保证物流的安全性和可靠性。

7. 征信平台加快建设

现代征信是指依法收集、保存和加工自然人、法人及其他组织的信用信息，并对外提供信用报告、评估和信息咨询等服务，帮助客户判断和控制信用风险，进行信用管理活动。将区块链技术与征信相结合，就可能在保持征信数量大、速度快、来源广等优点的基础上，弥补其数据的真实性、准确性不足的问题。当前，区块链在我国征信领域的应用已经受到了业界的高度关注，行业组织也相继成立，在区块链技术服务公司和征信企业的共同推动下，区块链征信平台的研发取得了一定成果，部分平台已经开始上线运营。

8. 工业应用重点探索

区块链在物联网、工业互联网、工业互联网平台等领域深度融合发展，将成为区块链在工业、制造业领域的主要应用形式。区块链在工业领域的应用主要集中在物联网平台、工业互联网平台、设备管理和安全等方面，具体包括智能制造、车联网、能源管理等领域。当前，国内知名企业包括阿里巴巴、京东、中兴、中国联通、万向以及其他初创企业正在积极探索区块链在该领域应用。

六、区块链技术落地情况

表 4 区块链企业典型应用案例表

应用领域	典型案例	企业
加密数字货币	中国人民银行积极开展针对国家数字货币的研究，成立了央行数字货币研究所，积极研究基于区块链技术的数字货币	中国人民银行
供应链金融	2018 年 12 月，蚂蚁区块链发布“双链通”，破局中小微企业融资难题	蚂蚁区块链
跨境支付与汇款	2018 年 8 月，中国银行通过区块链跨境支付系统，成功完成河北雄安与韩国首尔两地间客户的美元国际汇款	中国银行
医疗	2018 年 9 月 13 日,蚂蚁金服和上海复旦大学附属华山医院合作推出全国首个区块链电子处方	蚂蚁金服，上海复旦
资产管理	2018 年 9 月，金融壹账通发布了 ALFA 智能 ABS 平台，用区块链技术穿透底层资产，为场内外 ABS 发行提供解决方案	金融壹账通
溯源存证	2018 年 12 月蚂蚁金服“相互宝”首例互助案例使用区块链对参与者资料进行存证	蚂蚁金服
慈善	2018 年 10 月，贵州省扶贫基金会与 CROS 区块链技术公司携手合作的区块链智能公益平台正式上线	贵州省扶贫基金会，CROS 区块链技术公司
政府服务	2018 年 11 月 13 日，湖南娄底市联合湖南智慧政府打造了首个不动产区块链信息共享平台，它可以通过与其他部门进行共享和数据交互，完成对数据真实性评估，形成以不动产为中心的可信数据服务平台	湖南智慧政务区块链科技有限公司
物流	2018 年 3 月，腾讯公司与中国物流与采购联合会签署了战略合作协议，并联合发布了双方首个合作项目——区块链联盟链及云单平台，腾讯区块链正式落地物流场景	腾讯、中国物流
征信	2018 年 10 月 17 日，蚂蚁金服区块链携手华信永道打造“联合失信惩戒及缴存证明云平台”	蚂蚁金服
工业	2018 年 11 月 30 日，上海万向区块链股份公司、中都物流有限公司、星辰银行（中国）有限公司于上海联合宣布，基于区块链技术的“运链盟——汽车供应物流服务平台”正式上线	上海万向区块链股份公司、中都物流有限公司、星辰银行（中国）有限公司

区块链方案低成本解决了供应链金融价值传递问题。传统模式中，银行不愿给中小微企业提供授信，而区块链技术，凭借其可追溯特性和信用机制，可以帮 助这些企业获取应收账款融资。除此之外，银行还担心交易数据的真实性，供应链金融业务中核心企业以其 ERP 为中心化的模式串联上游采购信息和下游销售信息，由于核心企业的 ERP 系统结构较复杂，交易信息不易被篡改，所以银行对核心企业较为信任，但仍然担心核心企业与经销商或勾引商勾结篡改信息等行为，而区块链的特性则可以解决这些问题。供应链所有节点上链后，通过区块链的私钥签名技术，保证了核心企业等的数据可靠性；而合同、票据等上链，是对资产的数字化，便于流通，实现了价值传递。

版权保护问题突出，区块链有望在版权记录领域得到应用。传统版权行业具有三大痛点：作品版权难追溯，侵权行为难判断；利益归属难界定，原创作者权益难保障；维权成本高，举证困难。区块链上的数据具有时间戳，同时具有公开可追溯、不可篡改等特点，与数字内容在使用过程中的内容确权、合法传播，提升可信度等要求相符。传统数字内容的版权保护路径，需要创作者向国家授时中心及其下属的服务机构申请版权认证服务，门槛较高。但在区块链版权中，创作者或机构都可以通过加入区块链网络，快捷地实现内容上链，记录版权。

区块链应用优势：在信用证业务中应用区块链技术主要有以下几个优势。1. 去中心化：其没有中介机构，所有节点的权利和义务都相等，任一节点停止工作 都不会影响系统整体的运作。2. 去信任：系统中所有节点之间无需信任也可以进行交易，因为数据库和整个系统的运作是公开透明的，在系统的规则和时间范围内，节点之间无法欺骗彼此。3. 集体维护：系统是由其中所有具有维护功能的节点共同维护的，系统中所有人共同参与维护工作。4. 可靠数据库：系统中每一个节点都拥有最新的完整数据库拷贝，修改单个节点的数据库是无效的，因为系统会自动比较，认为最多次出现的相同数据记录为真。

医疗行业数据复杂，区块链解决数据安全问题。医疗产业产生众多数据，如患者医疗数据，临床数据，医保账单等。这些数据容易被攻击篡改，同时不够透明。区块链技术应用在医疗行业中，

可以保证这些数据的安全，减少当前医疗服务中介机构的摩擦成本。安全和不可篡改的信息储存。医疗领域饱受黑客袭击和勒索软件的困扰，安全的信息存储是医疗领域急需的。完全的运用区块链技术在医疗领域时，病人和医生便可以摆脱对黑客袭击的担忧自由的分享和交换医疗数据。与此同时，区块链技术可以让数据更加透明，医保和账单欺诈这些因为数据不 透明造成的损失数额高达百亿美元。运用区块链技术，所有数据都被加密签名，需要公私钥才可以进行查看，这可以极大减少欺诈的风险。

免责声明

本报告由中国银河证券股份有限公司博士后科研工作站向社会公开发布，是“博士后科研工作站专题研究报告”，不是证券分析师的分析报告。

本报告反映研究人员个人的不同设想、见解、论证及判断。本报告所载观点并不代表中国银河证券股份有限公司博士后科研工作站、不代表中国银河证券股份有限公司、也不代表我们的合作院校或任何其附属合作机构的立场，如果本报告出现政治或学术、技术性错误或失实情况由作者本人承担责任，与中国银河证券股份有限公司及其合作院校或任何其附属合作机构无关。

报告中的观点和陈述仅反映研究员个人撰写及出具本报告期间当时的分析和判断，本公司可能发表其他与本报告所载资料不一致及有不同结论的报告。本报告可能因时间或其他因素的变化而变化，从而导致与事实不完全一致的结论，敬请关注本公司就同一主题所出具的相关后续研究报告及评论文章。本公司、本报告研究人员及其附属机构不对任何因使用本报告或本报告所载内容引起的任何损失承担任何责任。

本报告中的观点和陈述不构成投资、法律、会计或税务的建议，本公司不就报告中的内容对最终操作建议做出任何担保。

本报告是“中国银河证券博士后科研工作站专题研究报告”，不是证券分析师的分析报告。本报告所载的全部内容只提供给阅读者做参考之用，并不构成对阅读者的投资建议，并非作为买卖、认购证券或其它金融工具的邀请或保证。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的银河证券网站以外的地址或超级链接，银河证券不对其内容负责。本报告提供这些地址或超级链接的目的纯粹是为了阅读者使用方便，链接网站的内容不构成本报告的任何部分，阅读者需自行承担浏览这些网站的费用或风险。

所有在本报告中使用的商标、服务标识及标记，除非另有说明，均为银河证券的商标、服务标

识及标记。

中国银河证券股份有限公司博士后科研工作站

简 介

中国银河证券股份有限公司博士后科研工作站（以下简称“工作站”），是经国家人力资源和社会保障部及全国博士后管委会批准设立的科研机构。

工作站以中国经济运行与发展中的重大理论问题、资本市场改革发展中的重大理论与实践问题和证券公司发展创新过程中的现实性、前瞻性、战略性问题为研究对象，以吸引、培养和储备高层次研究人才为己任，以提高中国银河证券综合竞争力、促进公司可持续发展、推进中国资本市场的理论建设为目标，力求通过宽视角、深层次、高质量的研究，为把中国银河证券打造成国内一流券商服务，为资本市场的改革发展服务，为发展繁荣中国的经济和金融科学服务。

为吸引高素质的博士毕业生进站从事研究工作，工作站为博士后研究人员提供在业内具有竞争力的、较高水平的工资和福利待遇，以及较为优越的科研条件和工作环境。