

## 证券研究报告—深度报告

### 信息技术

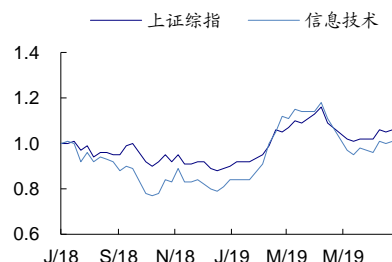
### 区块链行业专题报告

超配

(维持评级)

2019 年 10 月 27 日

#### 一年该行业与上证综指走势比较



#### 相关研究报告:

证券分析师: 熊莉

E-MAIL: xiongli1@guosen.com.cn

证券投资咨询执业资格证书编码: S0980519030002

证券分析师: 于威业

电话: 0755-22940920

E-MAIL: yuweiye@guosen.com.cn

证券投资咨询执业资格证书编码: S0980519050001

#### 行业专题

## 数字货币引领最强风口,区块链多元化应用场景进入落地期

### ● 区块链技术受到最高级别认可,成为核心技术自主创新重要突破口

在 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的集体学习会上,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作用,要把区块链作为核心技术自主创新的重要突破口。区块链技术再次受到权威认可,与产业应用相结合成为重点。

### ● Libra、IMFCoin 引发数字货币关注,质疑声下长期有望突出重围

近期 Libra 和 IMFCoin 的相关新闻将数字货币的关注度再度提升。但数字货币的发展仍面临较多反对的声音和问题。在一封公开信中,包括经济政策研究所和美国公共利益研究集团在内的 30 多个团体详细列出了 Facebook 加密货币 Libra 相关的一系列问题,这些问题涉及治理、国家主权、执法、税收政策、消费者保护、隐私、竞争和系统性风险。我们认为,由于数字货币独具交易便捷与费率低的特性,长期发展趋势或不会改变。未来伴随以上问题的逐步解决,基于区块链技术的数字货币由于具备安全性高、支付迅速、解决互信的特点,将成为国际化数字货币的主流形态。互联网巨头有望通过生态合作,在浪潮中充分受益。

### ● 区块链多元化应用场景逐步打开,市场边界不断拓展

区块链技术具备分布式、防篡改、高透明和可追溯的特性,非常符合整个金融系统业务需求,因此目前已在支付清算、信贷融资、金融交易、证券、保险、租赁等细分领域落地应用。而随着区块链技术的不断发展完善,应用也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。随着区块链的价值得到广泛的认可,越来越多的行业正在提出自己的区块链解决方案。

### ● 计算机行业上市公司纷纷布局,重点关注金融 IT 领域龙头公司

国家支持区块链行业发展,政策频出。2019 年国家互联网信息办公室正式发布第一批境内 197 个区块链信息服务备案编号。此次公布的第一批名单中包括百度、京东、腾讯、爱奇艺等互联网上市公司,也有金融或其他实体经济领域公司。上市公司方面,易见股份全资子公司易见天树和榕时代科技;安妮股份旗下版权家科技;晨鑫科技旗下竞斗云也进入首批名单。此次备案是监管部门依法对区块链行业进行规范的行政措施,同时体现了监管对区块链行业发展的鼓励,区块链行业逐步进入规范轨道。区块链当下重点在金融领域的应用需求较为迫切,建议关注布局区块链的上市公司:恒生电子、金证股份、易见股份、同花顺、航天信息等。

#### 独立性声明:

作者保证报告所采用的数据均来自合规渠道,分析逻辑基于本人的职业理解,通过合理判断并得出结论,力求客观、公正,其结论不受其它任何第三方的授意、影响,特此声明

#### 重点公司盈利预测及投资评级

公司代码	公司名称	投资评级	昨收盘(元)	总市值(百万元)	EPS		PE	
					2019E	2020E	2019E	2020E
600570	恒生电子	买入	74.99	54,991	1.09	1.40	68.87	53.47
600446	金证股份	买入	20.31	17,380	0.24	0.37	85.79	55.37

资料来源: Wind、国信证券经济研究所预测

## 内容目录

<b>区块链产业热度持续高涨，国内企业数量迅速上升</b>	<b>4</b>
区块链技术受到“最高级别关注”，与产业结合的应用是重点	4
区块链产业高速发展，企业数量快速增加	4
政策扶持，区块链技术备受重视	5
区域热度存在差异，产业分布呈集聚效应	6
应用多元化，覆盖多领域	7
三大数字货币交易平台交易规模较大	8
<b>区块链优势明显，保证数据真实性安全性</b>	<b>9</b>
数据传输真实性保密性使区块链备受青睐	9
去中心化有别于传统 IT 架构，提供安全保障	11
区块链安全性的根本，以比特币为例解析技术原理	13
区块链解决数据安全、人工成本等问题	18
<b>多领域应用区块链，颠覆传统模式</b>	<b>19</b>
基于区块链的数字货币呈快速发展之势——以 Libra 为例分析	19
区块链方案低成本解决供应链金融价值传递问题——以易见股份为例	25
版权保护问题突出，区块链应用提供司法证据	28
国际结算与跨境支付中高昂的费用问题，有望使用区块链解决	32
区块链有望解决电力产业链中发电、传输、交易、用户各端的互信问题	35
医疗行业数据复杂，区块链解决数据安全问题	36
<b>计算机行业上市公司纷纷布局，重点关注金融 IT、版权领域龙头公司</b>	<b>39</b>
<b>国信证券投资评级</b>	<b>41</b>
<b>分析师承诺</b>	<b>41</b>
<b>风险提示</b>	<b>41</b>
<b>证券投资咨询业务的说明</b>	<b>41</b>

## 图表目录

图 1: 2013~2017 我国区块链公司数量及增速图 .....	4
图 2: 2013~2018 我国区块链企业投资数量、融资金额统计图 .....	5
图 3: 中国区块链产业相关公司融资轮次分布情况 .....	5
图 4: 2018 年区块链创业活跃度省份情况 .....	6
图 5: 2018 年区块链创业活跃度城市情况 .....	6
图 6: 2018 年中国区块链产业细分领域公司和融资事件数 .....	7
图 7: 加密数字货币交易所 30 日成交额排行 (单位: 万美元) .....	9
图 8: 区块链基本运行原理 .....	9
图 9: 对称和非对称加密的原理简图 .....	10
图 10: 数字签名原理简图 .....	11
图 11: 传统中心化 IT 结构示意图 .....	12
图 12: 区块链的特性 .....	13
图 13: 比特币余额通过交易单推算 .....	13
图 14: 比特币交易单实现原理 .....	14
图 15: 哈希值变化使得原区块链断链 .....	17
图 16: 哈希值难以伪造 .....	18
图 17: 区块链中篡改数据产生数据分叉 .....	18
图 18: Libra 协会成员 .....	20
图 19: Basic HotStuff 算法流程 .....	21
图 20: Libra 支付示例图 .....	22
图 21: 2017.8.23-2019.6.26 比特币价格与成交量走势 .....	22
图 22: 比特币挖矿难度增大 .....	23
图 23: 基于区块链智能保理应用系统 .....	25
图 24: 区块链在供应链金融中应用步骤 .....	26
图 25: 区块链在供应链金融应用示意图 .....	26
图 26: 区块链+供应链金融业务逻辑 .....	27
图 27: 易见股份业务示例图 .....	27
图 28: 易见区块作为供应链金融解决方案的核心优势 .....	28
图 29: 2006-2016 年中国网络核心版权产业市场规模 .....	29
图 30: 区块链版权登记流程图 .....	29
图 31: 安妮股份版权区块链节点规划 .....	30
图 32: 安妮股份版权区块链应用具体场景 .....	30
图 33: 安妮股份版权区块链与天平链紧密对接 .....	31
图 34: 首个使用区块链证据进行判决的版权案件 .....	31
图 35: 传统的跨境转账涉及众多手续费环节 .....	32
图 36: 基于区块链的信用证系统物理架构 .....	33
图 37: 银行国际结算业务体系各交易主体结构简图 .....	33
图 38: 区块链跨境支付架构图 .....	34
图 39: 基于智能合约的电力市场交易模型 .....	35
图 40: 基于区块链的能源系统结构 .....	36
图 41: 医疗行业区块链应用示意图 .....	37
图 42: 医疗领域应用区块链示例 .....	37
表 1: 习近平主席强调要把区块链作为核心技术自主创新的重要突破口 .....	4
表 2: 区块链技术发展获得政策支持 .....	6
表 3: 区块链企业典型应用案例表 .....	7
表 4: 区块链企业典型应用案例表 (接上表) .....	8
表 5: 主流共识机制优缺点比较 .....	16
表 6: 目前区块链分类 .....	18
表 7: Libra 与支付宝, 微信支付和比特币的区别 .....	22
表 8: Libra 与传统数字货币的不同点 .....	24
表 9: 机构医疗信息安全与隐私保护区块链应用项目列表 .....	38
表 10: 计算机行业上市公司区块链布局梳理 .....	40

## 区块链产业热度持续高涨，国内企业数量迅速上升

### 区块链技术受到“最高级别关注”，与产业结合的应用是重点

中共中央政治局 10 月 24 日下午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作用。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。

区块链伴随着众多数字货币，一度饱受争议。但实际上，区块链在业内一直是一项极具价值和革命性的技术，其本质一种去中心化的数据库。随着此次会议的“认证”，相信区块链产业将会重新注入成长动力。在全球范围来看，我国在区块链技术的探索走在前列，拥有良好基础；同时，区块链技术能与人工智能、大数据、物联网等前沿信息技术的深度融合。本次会议对区块链技术进行了定位，目标要加强区块链标准化研究，提升国际话语权和规则制定权。区块链产业将大幅受益。

**表 1：习近平主席强调要把区块链作为核心技术自主创新的重要突破口**

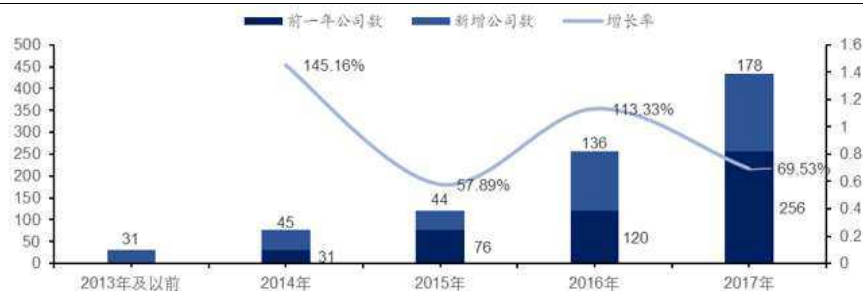
应用	主要内容
与基础技术融合	促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系
与实体经济融合	解决中小企业贷款融资难、银行风控难、部门监管难等问题
探索数字经济模式	为打造便捷高效、公平竞争、稳定透明的营商环境提供动力，为推进供给侧结构性改革、实现各行业供需有效对接提供服务，为加快新旧动能接续转换、推动经济高质量发展提供支撑
在民生领域的应用	推动区块链技术在教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用，提供优质公共服务
与新型智慧城市建设相结合	探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理的智能化、精准化水平
促进生产要素流通	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
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

资料来源:新华社, 国信证券经济研究所整理

### 区块链产业高速发展，企业数量快速增加

根据 2018 年中国区块链产业白皮书，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已经达到了 456 家，产业初步形成规模。2017 年是近几年的区块链创业高峰期，由于区块链概念的快速普及，以及技术的逐步成熟，很多创业者涌入这个领域，新成立公司数量达到 178 家。

**图 1：2013~2017 我国区块链公司数量及增速图**



资料来源：《2018 年中国区块链产业白皮书》，国信证券经济研究所整理

投资数量及融资金额大幅度上升。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。

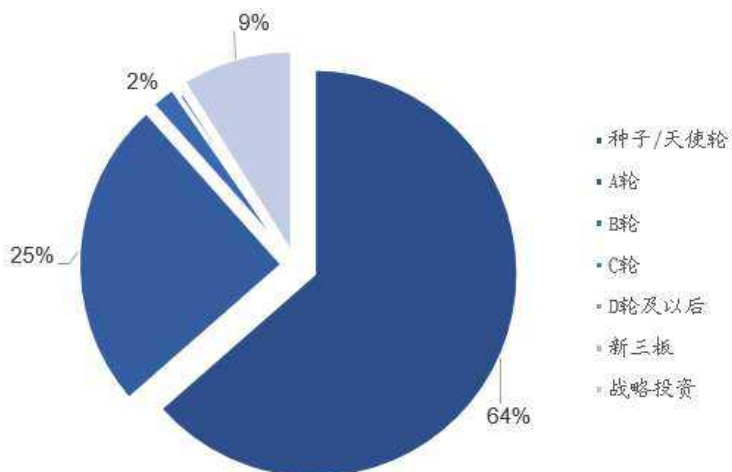
图 2：2013~2018 我国区块链企业投资数量、融资金额统计图



资料来源：前瞻产业研究院，国信证券经济研究所整理

区块链产业处于起步阶段。从中国区块链公司融资轮次分布状况来看，目前有接近 90% 的投资事件集中在早期阶段（A 轮及以前），另外有 9% 的投资事件属于战略投资 B 轮及以后的投资事件占比仅为 2%。因此，区块链产业目前还处于早期的阶段。

图 3：中国区块链产业相关公司融资轮次分布情况



资料来源：《2018 年中国区块链产业白皮书》，国信证券经济研究所整理

政策扶持，区块链技术备受重视



区块链技术日益获得政府的重视，政府陆续出台了许多政策推进区块链技术的发展及应用。从 2016 年 12 月国务院《“十三五”国家信息化规划》将区块链作为战略性前沿技术起，有关区块链的相关政策陆续出台，显示了政府对于发展区块链技术的决心和重视程度。同时在 ICO 监管方面，我国也已出台了相关政策加大对 ICO 项目的监管。

**表 2：区块链技术发展获得政策支持**

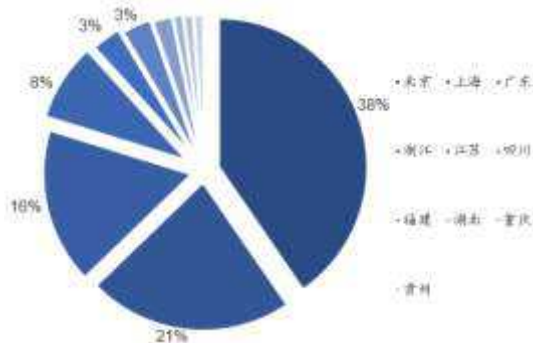
出台时间	政策名称/官方表态	政策/表态相关内容
2016 年 12 月	国务院《“十三五”国家信息化规划》	区块链首次被作为战略性前沿技术、颠覆性技术列入规划。
2017 年 1 月	工信部发布《软件和信息技术服务业发展规划（2016-2020 年）》	提出区块链等领域创新达到国际先进水平等要求
2017 年 1 月	商务部《进一步推进国家电子商务示范基地建设工作的指导意见》	推动示范基地创业孵化与科研院所技术成果转化有效结合，促进大数据、物联网、云计算、人工智能、区块链等技术创新应用。
2017 年 3 月	工业和信息化部印发《云计算发展三年行动计划（2017-2019 年）》的通知	通过举办创客大赛等形式，支持中小企业、个人开发者基于云计算平台，开展大数据、物联网、人工智能、区块链等新技术、新业务的研发和产业化，培育一批基于云计算的平台经济、分享经济等新兴业态，进一步拓宽云计算应用范畴。
2017 年 7 月	《国务院关于印发新一代人工智能发展规划的通知》	促进区块链技术与人工智能的融合，建立新型社会信用体系，最大限度降低人际交往成本和风险。
2017 年 8 月	商务部公安厅、财政部办公厅《开展供应链体系建设工作的通知》	重点推进二维码、无线射频识别（RFID）、视频识别、区块链、GS1、对象标识符（OID）、电子结算和第三方支付等应用，推动追溯系统创新升级。
2017 年 10 月	国务院发布《关于积极推进供应链创新与应用的指导意见》	研究利用区块链、人工智能等新兴技术，建立基于供应链的信用评价机制。
2018 年 3 月	工信部发布《2018 信息化和软件服务业标准化工作要点》	推动组建全国信息化和工业化融合管理标准化技术委员会、全国区块链和分布式记账技术标准化委员会。持续推进云计算和区块链等领域标准研制工作。支持在区块链参考架构、数据格式规范、互操作、智能合约等方向发布系列团体标准。
2018 年 6 月	工信部印发《工业互联网发展行动计划（2018-2020 年）》	开展工业互联网关键核心技术研发和产品研制，推进边缘计算、深度学习、增强现实、虚拟现实、区块链等新兴前沿技术在工业互联网的应用研究。

资料来源：各政府网站，前瞻产业研究院，国信证券经济研究所整理

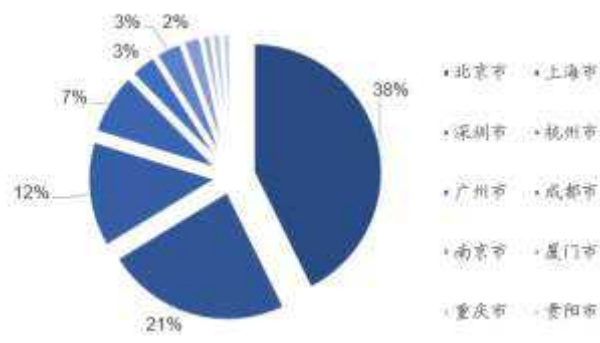
### 区域热度存在差异，产业分布呈集聚效应

根据 2018 年中国区块链产业白皮书，我国区块链技术公司分布较为集中，产业集聚效应明显，在共 456 家区块链相关产业公司中，北京、上海、广东、浙江四地合计占比超 80%，是区块链行业创业的集中地，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 21% 位居第二；广东省以 71 家公司、占比 16% 位居第三；浙江省以 36 家公司、占比 8% 位居第四。而从中国区块链创业活跃度靠前城市来看，北京、上海、深圳、杭州为中国大陆区块链创业活跃度最高的四座城市。占比分别为 38%，21%，12%，7%。

**图 4：2018 年区块链创业活跃度省份情况**
**图 5：2018 年区块链创业活跃度城市情况**



资料来源：《2018年中国区块链产业白皮书》，国信证券经济研究所整理

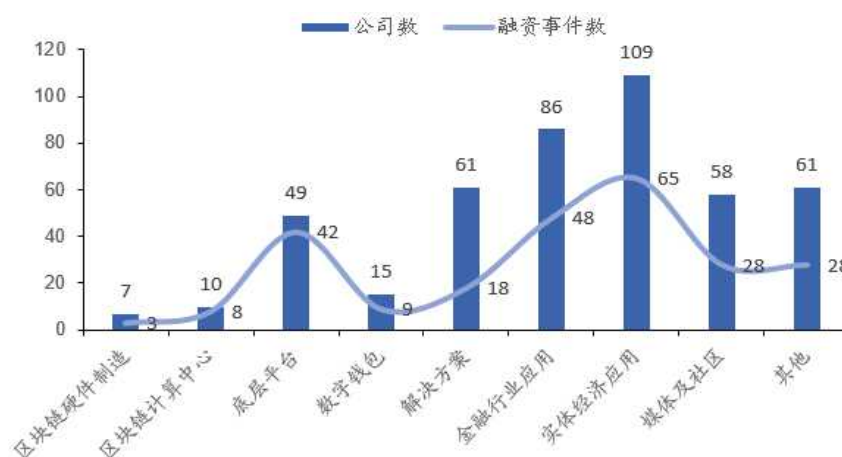


资料来源：《2018年中国区块链产业白皮书》，国信证券经济研究所整理

## 应用多元化，覆盖多领域

区块链产业新公司覆盖了多个领域，体现了区块链技术的应用多元化。根据《2018年中国区块链产业白皮书》，截至2018年3月底，区块链领域的行业应用类公司数量最多，其中为金融行业应用服务的公司数量达到86家，为实体经济应用服务公司数量达到109家。此外，区块链解决方案、底层平台、区块链媒体及社区领域的相关公司数量均在40家以上

图6：2018年中国区块链产业细分领域公司和融资事件数



资料来源：《2018年中国区块链产业白皮书》，国信证券经济研究所整理

区块链技术具备分布式、防篡改、高透明和可追溯的特性，非常符合整个金融系统业务需求，因此目前已在支付清算、信贷融资、金融交易、证券、保险、租赁等细分领域落地应用。而随着区块链技术的不断发展完善，应用也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。随着区块链的价值得到广泛的认可，越来越多的行业正在提出自己的区块链解决方案。

表3：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慧公益平台正式上线	贵州省扶贫基金会，CROS 区块链技术公司

资料来源：赛迪区块链研究所，国信证券经济研究所整理

表 4：区块链企业典型应用案例表（接上表）

应用领域	典型案例	企业
政府服务	2018 年 11 月 13 日，湖南娄底市联合湖南智慧政务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换，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，并联合发布了双方首个合作项目——区块链供应链联盟链及云单平台，腾讯区块链正是落地物流场景。	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、星展银行（中国）有限公司于上海联合宣布，基于区块链技术的“运链盟——汽车供应链物流服务平台”正式上线	上海万向区块链股份公司、中都物流有限公司、星展银行（中国）有限公司

资料来源：赛迪区块链研究所，国信证券经济研究所整理

### 三大数字货币交易平台交易规模较大

随着区块链技术的兴起和比特币的火爆，越来越多投资者进入币圈。目前国内三大数字货币交易所分别为火币网，OKEx 以及币安网。火币网自 2013 年创立以来，累积交易额突破 1 万亿美元，一度成为全球最大数字资产交易平台，占据全球 50% 数字资产交易份额。OKEx 是全球著名的数字资产交易平台之一，主要面向全球用户提供比特币、莱特币、以太币等数字资产的现货和合约交易服务。币安交易所是一个全球化的数字货币交易所，目前已获得泰国和迪拜的交易所牌照，并且已在瑞士、加拿大、美国、曼谷、迪拜等地设立运营中心。

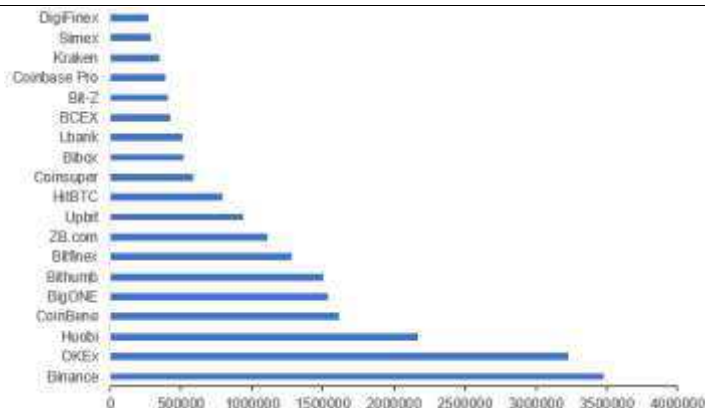
由于比特币的火爆，三大数字货币交易所每天成交额都很高，截止 2019 年 7 月 3 日 20 点，火币网 BTC/USDT 24 小时成交额约为 9.47 亿美元。OKEx 交易平台 BTC/USDT 24 小时成交量为 66468 BTC；币安网则为 11.6 亿美元。

根据 DAS Link 数据，截止 2018 年 7 月 31 日，加密数字货币交易所 30 日成交额最高的币安网，交易额达到了 350 亿美元，紧随其后的 OKEx 和火币网也有约 320 亿和 220 亿美元的成交额。数字货币市场交易量较大，投资者对



于数字货币投资拥有较高的热情度。

图 7：加密数字货币交易所 30 日成交额排行（单位：万美元）



资料来源：火币网，国信证券经济研究所整理

## 区块链优势明显，保证数据真实性安全性

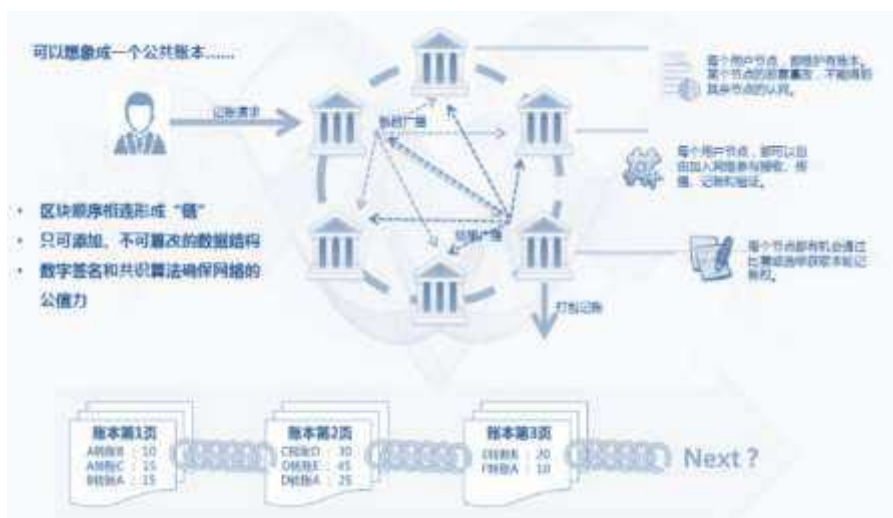
### 数据传输真实性保密性使区块链备受青睐

数据传输过程的中有两个基本问题：保密性、真实性。数据的传递需要保密，只能被适当的用户查看，此外还要保证传输数据的真实性，首先要保证数据发送者身份真实性，区块链技术以其公私钥非对称加密和数字签名技术保证保密性与真实性。

### 公私钥非对称加密技术保证信息传递保密性

如果把区块链想象成一个账本，区块是定时记录一部分数据的账单，区块相连成链。不同以往的中心化数据库，区块链账本是全网公开的，网络中的每一笔交易信息都向全网进行广播，每个节点都维护着全网全部交易记录的账本，并且每隔一段时间（10 分钟）进行对账更新。每个节点虽然拥有整个网络全部的信息，但是通过公私密钥非对称加密，只有拥有私钥的用户可以解读数据，其他节点只能如实记录却无从知晓内容，这就保证全网账单公开的同时保证了数据的保密性。

图 8：区块链基本运行原理

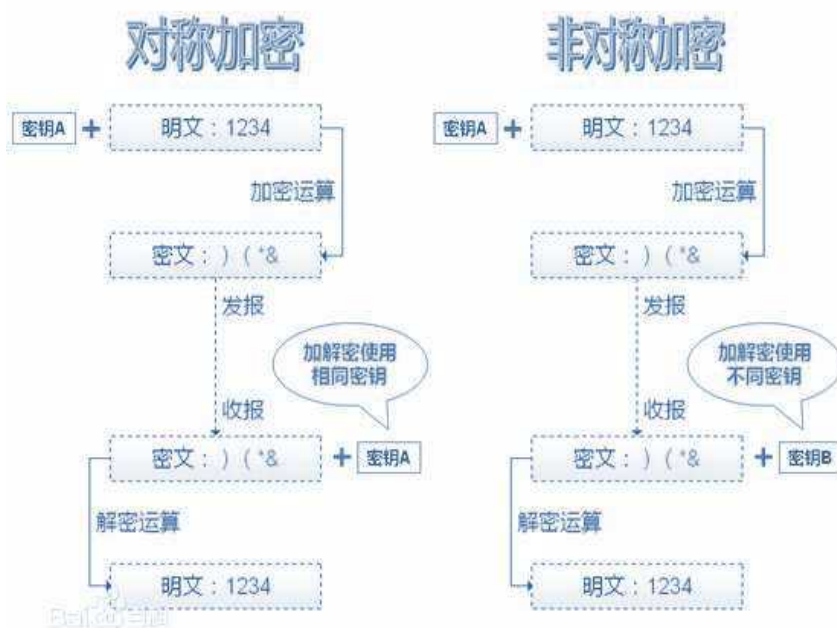


资料来源：云栖社区，国信证券经济研究所整理

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，而是经过加密的密文，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。

图 9：对称和非对称加密的原理简图



资料来源：百度百科，国信证券经济研究所整理

### 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，保证接收数据同发送数据完全一致是极其重要的，这就需要找到数据的“数字指纹”来唯一确定它。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

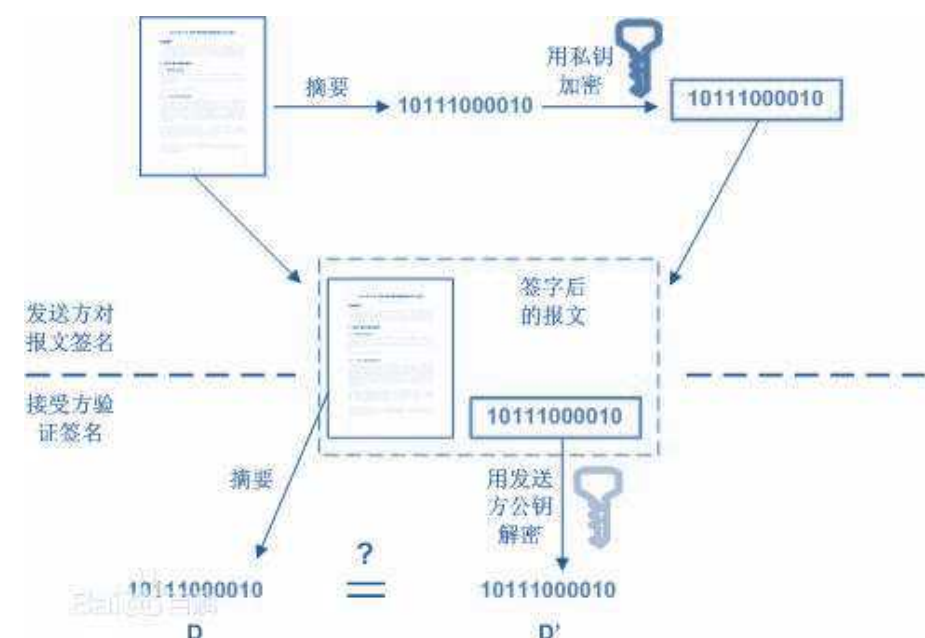
特征：1. 单向求解：你可以通过指纹确认一个人身份，但是指纹无法告知他的长相详细详细信息。同理，每个数据都有唯一的 Hash 值（“数字指纹”），通过原数据计算 Hash 值十分快，反向通过 Hash 值无法反推出数据全文。2. 强确定性：散列函数是一类函数的统称，如果用具体的某个散列函数（例如比特币区块中使用 SHA256 函数）对输入数据求解 Hash 值，一样的 Hash 值几乎一定对应完全一样的输入数据。这里用的是几乎一定而不是完全一定，因为在极小概率下，可以通过计算机穷举算出一个数据同伪造对象数据得出一样的 Hash 值，这样的计算叫做碰撞攻击。目前 SHA-0 和 SHA-1 存在碰撞攻击的方法，而 SHA-256 和 SHA-512 函数尚且不存在碰撞攻击的可能。所以，在目前用 SHA-256 算出一样 Hash 值的数据一定完全一样。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，则可以认为接收的数据和发送的数据完全一致未经篡改。

### 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。接收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。同时对数据求散列值，同解密后的散列值进行比对，如果二者相同，就证明数据是真实未篡改的。

图 10：数字签名原理简图



资料来源：百度百科，国信证券经济研究所整理

### 去中心化有别于传统 IT 架构，提供安全保障

区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。与传统的中心化 IT 架构最大的区别在于去中心化。

### 传统中心化 IT 架构存在一定弊端

中心化的设计思想很简单，分布式集群中的节点机器按照角色分工。中心节点负责分发任务并监督其他节点，若其他节点有空闲，则分配新任务，如果节点死亡，中心节点将剔除该节点并把原任务分配给新的节点。中心化的设计存在的最大问题是中心节点的安全问题，如果中心节点宕机，则会导致整个系统崩溃。而去中心化架构，联网的任意节点设备宕机，都只会影响很小范围的功能。

图 11：传统中心化 IT 结构示意图



资料来源：Java 架构师学习，国信证券经济研究所整理

除此之外，中心化结构灾备成本更高。当中心节点被攻击或宕机时，整个系统崩溃，则需要建立另一个灾备系统，成本将升高。而去中心化每个节点高度自治，任何一个节点都可能成为阶段性的中心，同时去中心化架构将数据存储在分布式节点网络上的数千个设备中，所以系统和数据对于技术故障和恶意攻击都具有很强的抵抗性。若单个节点故障或脱机，网络的可用性和安全性也不会受到影响。

中心化结构保障信息安全能力较差。中心化结构中，若中心节点被攻击，全部信息将丢失或被篡改。而去中心化架构中，每个节点都可以存储信息，可以较大程度保证信息安全。

但由于去中心化需要每个节点达成共识，而达成共识所需要的时间将会随着节点数量增多而增大；中心化由一个中心节点分配监督，相对去中心化架构而言有更高的效率。

### 安全与信任使区块链获得瞩目

安全是指数据不会被篡改或者毁灭丢失，中心化 IT 架构一旦中心节点被攻占或者宕机，数据极易被篡改或丢失，数据的安全性得不到很好的保障。同时，中心化架构中的数据对公众是保密的，对中心节点是透明的。公众信任中心节点会如实记录数据，不会做出有利于自身而不利公众的篡改，这就是信任。信任一般来自于权威第三方的背书，银行由政府背书。然而在权威部门尚未形成的领域，对数据真实性的判别几乎无法达成，因为信任尚未建立；其次。中心节点永久掌握了记账权，导致其它易腐化，信任危机与信任重塑不断的周而复始更替，带来巨大的损失。

### 区块链四大特性：去中心化、去信任、计提维护、可靠数据库

区块链有以下四个主要的特性：去中心化(Decentralized)、去信任(Trustless)、集体维护(Collectively maintain)、可靠数据库(Reliable Database)。并且由四个特性会引申出另外 2 个特性：开源(Open Source)、隐私保护(Anonymity)。

去中心化(Decentralized)——分布式存储与对账：各节点记账并储存，每个节点都遵循同一记账交易规则，而该规则基于密码算法而非信用，同时每笔交易需要网络内其他用户的批准(相当于验算)，不需要第三方中介结构或信任机构背书。在传统的中心化网络中，对一个中心节点(例如支付中介第三方)实行有效攻击即可破坏整个系统，而在一个去中心化的例如区块链的网络中，攻击单个节点无法控制或破坏整个网络。

去信任(Trustless)——交易技术性执行：参与整个系统中的每个节点之间进



行数据交换是无需互相信任的，整个系统的运作规则是公开透明的，系统内交易批准取决于所有节点共识性原则，规则对于所有节点公平且强制。所有的数据内容也是公开的，因此在系统指定的规则范围和时间范围内，节点之间是不能也无法欺骗其它节点。

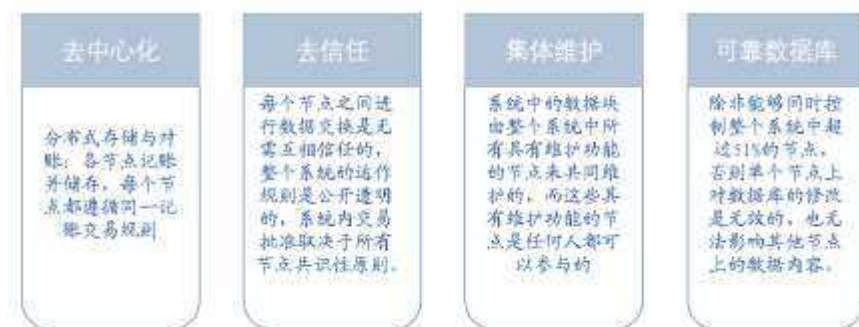
**集体维护 (Collectively maintain):** 系统中的数据块由整个系统中所有具有维护功能的节点来共同维护的，而这些具有维护功能的节点是任何人都可以参与的。

**可靠数据库 (Reliable Database):** 整个系统将通过分数据库的形式，让每个参与节点都能获得一份完整数据库的拷贝。除非能够同时控制整个系统中超过 51% 的节点，否则单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容。因此参与系统中的节点越多和计算能力越强，该系统中的数据安全性越高。

**高度透明 (Open Source):** 由于整个系统的运作规则必须是公开透明的，所以对于程序而言，整个系统必定会是开源的。

**匿名隐私保护 (Anonymity):** 由于节点和节点之间是无需互相信任的，因此节点和节点之间无需公开身份，在系统中的每个参与的节点的隐私都是受到保护的。

图 12: 区块链的特性



资料来源：国信证券经济研究所整理

## 区块链安全性的根本，以比特币为例解析技术原理

区块链中的数据是可检索、不可篡改的，实现主要依靠两大设计：数字签名、共识机制（记账权分配）。区块链技术是比特币的基础，比特币是对区块链技术的第一个成熟的应用，比特币借助区块链解决了传统信用货币体系下的交易造假、双花（double spend）问题。

（一）比特币世界概述：比特币体系中不存在单独货币，只存在交易单，每个人有自己的账户 ID，每一次交易，获得多少钱，花多少钱，全以交易单形式记录在账单上，货币值是依附于交易单存在的，余额通过追溯累计所有其参与的交易单就可推算得出。

图 13: 比特币余额通过交易单推算



Contents of a Bitcoin Wallet



资料来源：牛币辞典，国信证券经济研究所整理

每页账单只记录比特币全世界 10 分钟内的交易信息。每 10 分钟一个新的账单被产生（制造/创建）出来，所以账单随时间流逝会不断增多。每个人每做一笔交易，某页账单上就会记录这笔交易单。这个记录过程是比特币软件通过网络自动完成的（黑客很难伪造）。目前比特币世界存活了 4 年多，就有大概 24 万多页账单了。（4 年\*365 天\*24\*60 分钟/10 分钟=21 万页账单）。账单放在全世界唯一的账本上，账本上会全部的交易单，并且网络中每个用户有一本。只要账本上收支都记录清楚，这个世界不需要单独货币也可以做交易（等于大家都刷卡交易）。账单就是区块，账本就是区块链。

（二）如何交易：——数字签名防伪。比特币的交易是通过签写交易单（Tx）完成的，例如 B 从 A 处获取的 10 个比特币，想用它们购买 C 的 pizza，B 需要写一个交易单，并向全网广播，具体的交易流程如下：A 从某处（X）获得了 10 个比特币记录在 Tx0，A 转账给了 B，记录在 Tx1，B 转账给 C，记录在 Tx2。每个交易单都是进出双向记录的，类似于会计上的复式记账法。来源（In）记录本次转账资金的来源，有两个科目：上一次交易单 ID（上次交易单全文 Hash 值）、上次发送方的数字签名。去向（Out）记录本次转账资金的去向，主要包含三个科目：转账金额、接收方公钥、发送方的数字签名（加密资金来源交易单+接收方公钥生成的 Hash 值）。

每个节点收到 Tx2 之后进行如下验证：

- 1，通过 ID 找到 Tx1 交易单
- 2，获得 B 公钥
- 3，用 B 公钥对 Tx2 数字签名解密
- 4，比对 Hash 来验证

验证可以得出两个结论：

- 1，B 确实从 A 获得了 10 个比特币（Tx1 上有 A 的数字签名）
- 2，B 确实要 C 10 个比特币，因为（Tx2 上有 B 的数字签名）

交易的真实性得到保证，交易造价被杜绝！

图 14：比特币交易单实现原理



资料来源: 国信证券经济研究所整理

### (三) 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, 网络传输情况不同, 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, 所以有必要都进行一下介绍。

**表 5：主流共识机制优缺点比较**

共识机制	优势	缺点
PoW	实现简单，不需要过度复杂代码。 容易控制哈希值正确性。 系统可以承受大量节点。	消耗非常多的能源。 共识时间长。
PoS	资源消耗少	更多的安全问题。 实现较复杂。
DPoS	资源消耗少。 共识时间短。 吞吐量高	中间步骤较多，容易产生安全漏洞。 拥有高权益的参与者可投票使自己成为一名验证者
PBFT	可脱离币的存在 共识效率高	有 1/3 或以上记账人停止工作后，系统将无法提供服务。
dPoW	节能 安全性高 添加价值到其它区块链，无需付出 Bitcoin（或是其它任何安全链）交易的代价	只有使用 PoW 或 PoS 的区块链，才能采用这种共识算法 “公证员激活”模式下，必须校准不同节点（公证员或正常节点）的哈希率
dBFT	快速；可扩展	可能存在多个根链
PoET	参与代价低，去中心化。 易于验证领导者是通过合法选举产生的。	必须要使用特定的硬件； 不适用于公有区块链
LibraBFT	具有三分之一的容错性，防止双花攻击 吞吐量高 稳定性较强	星形拓扑结构通信中间节点被攻击可能造成全网瘫痪

资料来源：币世界，区块链，区块链大本营，国信证券经济研究所整理

### 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，验证通过之后就以后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）

### 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具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 1 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= $3000 \times 5\% / 365 = 0.41$  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，验证通过之后就以后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。

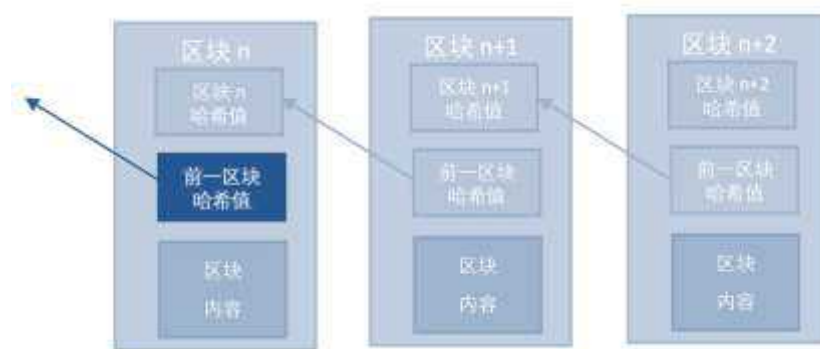
比拼核心：愿意支付的币龄（自己给自己转账的金额）

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。

图 15：哈希值变化使得原区块链断链



资料来源：冰河杂谈，国信证券经济研究所整理

#### （四）如何成链：——共识机制（侧链消除）

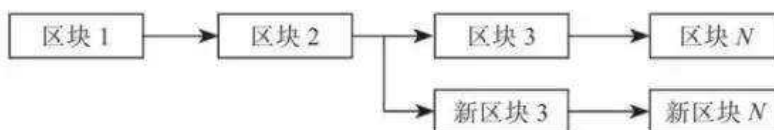
区块排列：传统账单的页码是连续的数字，而区块链账单的页码是前十位数字为 0 的超长随机数密码（Hash 哈希算法生成）。在区块链账单中，需要指定上一页的页码，才能将区块有序排列。每一个区块是使用密码学签名与下一个区块‘链接’起来的。区块头中的“本区块哈希值”相当于账单的“本页页码”，“父区块哈希值”相当于“上页页码”。而“页码”的具体数值是使用上一页“正文”的全文作为自变量，通过哈希函数生成的随机字符串。网络里的计算机要争夺记账权，就必须随机生成到前十位数字是 0 的“页码”，而随机数的前十位为 0 是个极端罕见的事件，因此整个区块链网络也需要花 10 分钟左右的时间，才可能由某台计算机找到一个这样的“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）

图 16: 哈希值难以伪造

版本	1	
前一区块哈希值	0000000000000000015bd6a04efb06d2a1a1b0f1c5a42b3da0b4f1e6f48a1a1f	
默克尔树根	1e2790419058e27b6e690d6f230a44bf153885fe41fd00c9156475b49a488a0a	
时间戳	1531353835	
难度系数	5,363,678,461,481.36	
随机数	224885659	
交易数量	133	
CoinBase 交易		
其他交易		

**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（如图所示）。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。

图 17: 区块链中篡改数据产生数据分叉



## 区块链解决数据安全、人工成本等问题

根据节点网络的可进入性和记账权的分配规则，区块链分为公有链和私有链。公有链中的节点可以任意进出，完全公开。私有链分为混合和完全两种，混合私有链指定多个记账节点，其他节点只参与交易不参与记账，完全私有链仅仅使用区块链的总账技术进行记账，与其他的分布式存储方式没有区别。

表 6: 目前区块链分类

	公有链	联盟链	私有链
参与者	任何人自由进出	联盟成员	个体或公司内部
记账	每个人都可以竞争记账权	记账权并不公开，且只记录内部的交易	预先指定几个节点为记账人，每个区块的生成由所有预选记账人共同决定，其他节点可以交易，但是没有记账权。

区块链本质上是**通过牺牲速度和 IT 资源来换取公平性**。拥有优势包括安全，减少人工、结算、交易成本，利用闲置硬件资源等。



## 多领域应用区块链，颠覆传统模式

区块链技术具备分布式、防篡改、高透明和可追溯的特性，符合融系统业务需求，在数字货币、供应链金融、跨境支付等细分金融领域落地应用。而随着区块链技术的不断发展完善，应用也从金融领域延伸到实体领域，越来越多的行业例如电力、医疗、版权保护等，区块链解决方案也获得初步应用。

### 基于区块链的数字货币呈快速发展之势——以 Libra 为例分析

#### 数字货币仍面临较大争议

数字货币已历经长时间的探讨，近期 Libra 和 IMFCoin 的相关新闻将数字货币的关注度再度提升。但数字货币的发展仍面临较多反对的声音和问题。

Facebook 于 2019 年 6 月 18 日晚发布了其加密货币 Libra 的白皮书和官方网站，中文名称为“天秤座”，引起了轩然大波。根据白皮书，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。

而在 7 月 3 日，据 CNET 报道，在一封公开信中，包括经济政策研究所和美国公共利益研究集团在外的 30 多个团体，呼吁美国国会和监管机构叫停 Facebook 的加密货币 Libra 项目，直到相关的“深刻问题”得到解决。在一封公开信中，他们详细列出了与 Facebook 加密货币相关的一系列问题，这些问题涉及治理、国家主权、执法、税收政策、消费者保护、隐私、竞争和系统性风险。他们写道：“我们呼吁美国国会和监管机构叫停 Facebook 的加密货币 Libra 及其相关计划，直到相关的深刻问题得到解决。”在公开信中，这些团体表示：“美国的法规系统还没有准备好解决这些问题，其他国家或国际机构的法规系统也还没有准备好。”一些议员也呼吁 Facebook 暂停对 Libra 的开发，理由是该公司似乎有没完没了的丑闻。这与众议院金融服务委员会主席玛克辛·沃特斯的类似要求相呼应。她的小组和参议院的对应小组计划在 7 月就 Libra 问题举行听证会。

此外，国际货币基金组织（IMF）与世界银行近期发布联合报告，通过 96 个参与调查的成员国家的反馈，探讨了金融科技对全球经济及货币体系带来的影响。报告称，“央行支持的数字货币或成为现实”，调查中 20% 的反馈机构称正在探索发行央行数字货币的可能性，不过这些工作都在早期阶段，仅仅有四个被报道的测试项目。该报告发布之后，被部分区块链媒体解读为“IMF 拟发行全球数字货币 IMFCoin”。实际上，2017 年年底已经有媒体曾经推测并炒作过“IMF 拟发行全球数字货币 IMFCoin”的新闻，当时在 2017 年 9 月，国际货币基金组织（IMF）总裁克里斯蒂娜·拉加德在英格兰银行庆祝独立 20 周年的活动上发表了题为“中央银行业务和金融科技——美丽的新世界？”的演讲，之后被众多媒体解读为她暗示该组织拟根据特别提款权（SDR）机制，推出一个类似比特币的全球数字货币 IMFCoin，“旨在取代现有储备货币”。此次联合报告，再次激发关于“IMFCoin”的猜测。

#### 曲折的发展背景下，数字货币独具便捷与费率低的特性，发展趋势或不会改变

Libra 拥有的最大的优势是全球化和手续费低。Libra 实现的全球化和低手续费的特点可以一定程度解决人们开立银行账户困难，且交易手续费高的痛点，同时基于区块链的反篡改，反洗钱特点，可以良好保护资产安全性并携手监管机构提高反洗钱的效力。

根据白皮书，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。对 Libra 的通俗理解是一个基于去中心化区块链技术的加密数字货币。Libra 去中心化治理，由 Libra 协会（非盈利组织）进行管理。

图 18: Libra 协会成员



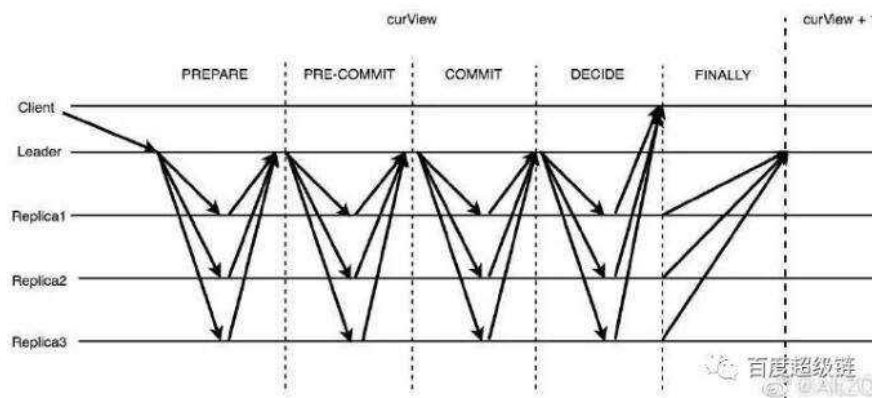
资料来源: Libra 白皮书, 国信证券经济研究所整理

**Libra 以区块链为基础架构。**Libra 目前采用的是联盟链, 具备高性能和安全隐私。Facebook 选择自行开发了区块链基础设施以进行 Libra 的记账。目前由于技术限制和安全考虑, Libra 采用的是联盟链的形式, 只有受许可的成员才能成为节点。初期目标是招募 100 个验证节点, 达到每秒 1000 笔交易。Libra 区块链一大特点是其为开源的, 开发者可以基于 Libra 区块链开发自己的应用, 代码可从 github 上获得。

在账本表示方面, 与当前大多数区块链系统类似, 采用了账户余额模式, 而不是比特币的 UTXO 模式。在账本底层, 虽然 Libra 同样采用了 Merkle 树来校验数据, 但可能并没有传统意义上的“区块+链”式的底层数据结构。因此 Libra 的账本更像是一系列账本状态的历史集合记录。Libra 随着系统的不断使用, 账本总容量也会不断加剧。Libra 在白皮书中也表示未来可能会设计资源租赁等机制来解决这个问题。

在共识机制方面, 当前协会成员为 Libra 区块链的验证节点, 新设计了 LibraBFT 的共识机制, 是基于另一个近期备受关注的 BFT 共识 HotStuff, 并做了若干修改, 实现所有验证者节点就将要执行的交易及其执行顺序达成一致。这种方法可以在网络中建立信任, 因为即使某些验证者节点(最多三分之一的网络)被破坏或发生故障, BFT 共识协议的设计也能够确保网络正常运行。与其他一些区块链中使用的“工作量证明”机制相比, 这类共识协议还可实现高交易处理量、低延迟和更高能效的共识方法。

图 19: Basic HotStuff 算法流程



资料来源：百度超级链，国信证券经济研究所整理

Libra 区块链采用 Rust 语言进行编写。Rust 语言具有较高的安全性和易用性，通过所有权系统管理内存，在运行时，所有权系统的任何功能都不会减慢程序，所以其编写的区块链通常具有较强的性能。而对于 Libra 智能合约，Libra 自创了 Move 编程语言，用于在 Libra 区块链中实现自定义交易逻辑和“智能合约”。Move 是一种静态类型语言，而从本质上来说这其实是一种编程逻辑上的约束，因此要比以太坊的智能合约语言要严格得多。类似 Rust、Golang、Typescript、Haskell 或 Scala 等现代编程语言均为静态类型语言，因为许多简单的程序 Bug 可以在编译的过程中就被检测出而不是等到执行程序的时候才被发现。

Move 语言中的另一个特色是技术文档中提到的“First-class Resources”，即“一等资源”，这里的“资源”和以太坊编程语言中的“Value”（值）是对应的概念，不同点在于“值”可以被随意复制，而“资源”则只能被消耗。Move 的设计考虑到了其金融的应用场景，对于数字资产的相关操作进行了模块封装，并设计了可以进行灵活的权限控制的接口。Move 合约在设计时，充分考虑了安全性，能够解决合约重入漏洞。此外 Rust 和 Move 语言都采用的是静态类型系统，让类型检查在编译的时刻进行，能减少了运用时的 bug，增强系统的安全性。

Libra 拥有的最大的优势在于全球化和手续费费用低。Libra 实现的全球化和低手续费的特点可以一定程度解决人们开立银行账户困难，且交易手续费高的痛点，同时基于区块链的反篡改，反洗钱特点，可以良好保护资产安全性并携手监管机构提高反洗钱的效力。数字加密货币并不像传统数字货币一样受到政策和区域的影响，只要有互联网接入，区块链能够连接，就可以通过区块链进行转账，使得 Facebook Libra 具备了全球货币的特性。无论是跨国转账，还是跨境支付，都能轻松实现。在区块链系统中，每发行一枚数字加密货币（又叫 Token 或者 Coin），都会在区块链上进行记录。这样可以解决货币超发，滥发的问题。

Libra 是基于区块链的跨境支付过程的价值载体，在有万亿美元市场规模的跨境支付市场，可以提高效率并降低成本，实现“交易即结算”。其次 Libra 可以作为投资人的投资工具，在未来的金融领域中，可能可以扮演重要角色。

Libra 的应用场景广泛。从 Facebook 公布的合作伙伴名单我们可以看出这一稳定币的主要用途是支付。用户可以直接买入 Libra 稳定币，然后通过 Facebook 或者 Paypal 等渠道进行花费，它可以用于在 eBay 购物、可以进行投资、可以充话费，也可以用于支付打车费用等等类似于其他货币的应用场景。

图 20: Libra 支付示例图



资料来源：币策财经，国信证券经济研究所整理

**Libra 与支付宝和微信支付的区别。**Libra 与国内支付宝和微信支付有着不一样的特点。微信支付和支付宝主要分两块，一块是便捷的操作体验，也就是支付工具；另一块是个人的网络账户，而 Libra 可以兼顾这两种功能，同时，Libra 拥有一个最重要的底层支持：货币发行权。Libra 的推出有学习腾讯阿里支付的影子，只是它更全球化。它与体外法币（美元，欧元）稳定兑换，广告商支持美元购买 Libra，用于支付在 Facebook 的广告费，用户 A 也可以把得到的以 Libra 计量的优惠券转送 B，这个特点很像 Q 币。

表 7: Libra 与支付宝，微信支付和比特币的区别

类型	发行方	发行模式	价值锚	兑换	清算
Q 币	腾讯	用户购买	兑换腾讯公司服务	腾讯	腾讯
支付宝	支付宝	用户充值	1: 1 兑换人民币	银行	支付宝
Libra	Libra 协会	用户充值	1: 1 兑换一篮子货币	Libra 会员	区块链
比特币	POW 协议	数字计算	买卖供需	交易所	区块链

资料来源：币策财经，国信证券经济研究所整理

**Libra 作为一种数字货币，与比特币具有较大区别。**数字货币是电子货币形式的替代货币。数字金币和密码货币都属于数字货币。可以认为是一种基于节点网络和数字加密算法的虚拟货币。目前数字货币的三大特点：交易成本低，交易速度快和高度匿名性。如今随着比特币的火爆，有多种数字货币相继发行。目前较为出名的有比特币（Bitcoin），以太坊（Ethereum），比特币现金（Bitcoin Cash），瑞波币（Ripple）以及莱特币（Litecoin）。近年很多数字货币都获得了巨大成功，其中以比特币为例，比特币获得成功的因素包括高度虚拟化，安全性高，支付迅速，解决互信问题。

图 21: 2017.8.23-2019.6.26 比特币价格与成交量走势



资料来源：汇金 110，国信证券经济研究所整理

首先比特币基于区块链技术，通过挖矿来发币，是一种高度虚拟化的货币，比特币使用整个 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，并使用密码学的设计来确保货币流通各个环节安全性。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。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。

与此同时，比特币的交易相当迅速，通常比特币账户发起一笔交易后，在几秒



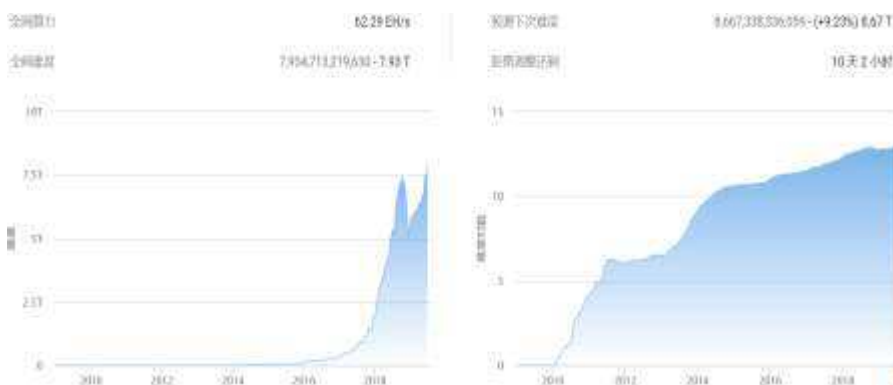
钟内就能收到来自全球范围内的确认，大约一小时后这笔交易就可以被认为是安全完成了。

比特币还解决了信任问题，比特币建立信任，因为它的交易历史将由多个独立节点记录，任何一方都无法轻易修改。比特币账本的数据是公开透明的。因为在比特币网络中不会存储任何私密信息，所以所有人都能够看到账本中的全部数据。任何时间，任何地点，只要有网络接入比特币，就能够查看比特币历史上所有的交易。

强大的计算能力是比特币存在的保障。PoW 算法的特点是受到 51% 的攻击就可以篡改数据，控制网络中的交易。2012 年 1 月份，当时市场上的 token 除了 BTC 以外基本上大多都是 BTC 的山寨币，完全模仿抄袭 BTC 的代码，这也是第一批‘山寨币’一个名为 Coiledcoin 的山寨币，算法是和 BTC 相同的 Sha-256 算法，项目刚上线就被 BTC 的社区成员联合矿池进行了 51% 攻击，最后基本消失。比特币强大的计算能力保证了其经久不息。

最后，比特币成功的炒作让其拥有了大量用户，对接方数量多，而其本身货币量少，供应上限共只能开采 2100 万个币，这种稀有性也使得比特币价值涨高。

图 22: 比特币挖矿难度增大



资料来源: BTC.com, 国信证券经济研究所整理

通过比特币的例子，可以发现数字货币需要具备的特性包括交易迅速，计算能力强，安全性高和多的接手方。紧随比特币身后的莱特币，以太坊，瑞波币等均等拥有这些特性。

**Facebook 发行 Libra，目标成为全球支付手段。**Facebook 作为互联网巨头发行了 Libra 这一全球性数字货币，结合前文论述的数字货币成功要素，可以看到发行 Libra 这种全球性数字货币的企业需要具备以下的特点：大基数的全球用户，强大的技术支持，监管的支持以及强大的影响力。首先需要有庞大基数的全球用户，Libra 旨在成为全球化的用于支付的数字货币，这就需要拥有高数量的用户作为基础，而 Facebook 作为全球网络巨头，全球拥有超过 25 亿用户，这一庞大的用户基础使得 Libra 的使用有了保障。其次是强大的技术支持。根据上文所述数字货币成功要素可以了解到数字货币要保证数据不受攻击不被篡改，需要有强大的运算能力，而 Facebook 作为互联网巨头，拥有强大的技术支持。第三点需要有监管的支持。Libra 是锚定一篮子货币的数字货币，具有真实的价值储备，然而发行者是私人企业，这就需要得到监管的支持。最后是需要有强大的影响力。Facebook 在发布 Libra 的消息后，全球范围引起广泛热议，Libra 协会由众多行业巨头组成，为 Facebook 提供支持。以成为全球支付手段作为目标，强大的影响力是 Facebook 不可或缺的因素。

**Libra 与传统数字货币存在相同点也有不同的特征。**Libra 同样是基于区块链技



术，去中心化的数字货币，拥有交易快速和交易成本低特征。同时在价值波动，匿名性，节点验证等方面有着不同。这些不同点，有望促使 Libra 成为真正意义上的世界性数字货币。

表 8: Libra 与传统数字货币的不同点

不同点	Libra	传统区块链数字货币
价值波动	根据一篮子货币的价值，对于其他法定货币有着一定的汇率，所以价值波动远小于传统数字货币。	没有锚定货币，传统数字货币的价值波动较剧烈。
匿名性	符合反洗钱条例，交易需要通过 KYC 验证，并由 Libra 协会进行监管。	匿名性交易
节点验证	至少在头五年将基于“许可节点验证”对每笔交易的验证只能由建立网络的内部人员来完成。唯一能够核实交易的内部人士将包括 Libra 协会中的成员。 每项交易的验证都只能由 Libra 协会的成员进行。	多为全节点
发币模式	当一个正常的国家货币被用来购买 Libra 时，Libra 产生。 Libra 协会是唯一能够创造（铸币）和毁灭（燃烧）Libra 的一方	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）等共识机制
可否支付	全球范围内实行交易，支付购买商品，使用者通过 Calibra 电子钱包直接进行交易	需要找接手方进行交易，兑换国家主权货币，进而进行支付
用途	主要用于支付	多用于投机

资料来源：美股研究社，国信证券经济研究所整理

数字货币的推广有望对传统银行的经营模式产生影响。由于数字货币的特有优势，对支付体系和银行体系形成了巨大的冲击。作为支付系统与金融市场基础设施的监管者，以及支付系统研发和创新的催化剂，中央银行有责任提高支付系统的安全性和有效性。数字货币对第三方支付有强烈的冲击，不仅仅表现在数字货币交易模式的内生优势，更是在数字货币加速脱媒对第三方支付的冲击、替代第三方支付的传统增值服务以及与银行账号结合对第三方支付产生的挑战。数字货币能够完成自主的去中心的清算、分布式的记账和离散化的支付，所以客户在交易、记账和最后清算中都没有必要再经过银行。随着数字货币的使用越广泛，银行的清算业务、支付结算业务等都将不会再被需要。不过在当前大数据时代背景下，失去这些业务不仅仅只是损失办理这些业务的手续费，重要的是失去了大量客户的交易记录和交易数据，因而失去这些数据中潜伏各种商业机会，也就失去了掌握经济发展全局的战略制高点。同时数字货币如果大规模使用，必定对法币也造成一定影响，减少持有的法定货币将会对银行传统业务的存款造成冲击，而存款业务又是负债业务最重要的部分。这对传统经营模式的银行形成巨大冲击。

Libra 打破主权货币限制，或有望冲击世界货币体系。Facebook 的这次举动本质上是互联网企业依靠自己的科技和覆盖广度，扮演起世界央行的角色。随着 Libra 的发行，国际结算中使用的货币，支付使用的货币，金融资产选择的货币等都可能偏好 Libra，这将对现有货币体系产生巨大的冲击。现有货币，尤其是崛起中的主权货币会面临跨维度的挑战。作为世界货币体系中的主要组成部

分，由各国央行发行的主权信用货币具有明显的主权界限，用户在使用过程中也存在诸多限制。而 Libra 的愿景，就是成为一套简单的、无国界的低波动性的数字货币。在现有货币体系内，也出现了推动超主权货币的努力。在 2009 年 G20 会议上，时任中国人民银行行长的周小川提出“创造一种与主权国家脱钩并能保持币值长期稳定的国际储备货币，从而避免主权信用货币作为储备货币的内在缺陷”。基于区块链发行的 Libra，打破了传统意义上的主权界限，不受任何主权国家的独立监管，并对用户不具有排异性。从这方面来看，Libra 与超主权货币存在诸多类似之处。

如果 Libra 很受欢迎，人们就会把他们的国家货币如美元、欧元、人民币和卢比等兑换成这种新的数字货币，以便买卖许多以 libra 定价的产品。许多用户可能会选择保留 libra，而不是兑换回本国货币。因此，Facebook 或 Libra 协会将继续持有多个国家的货币，并通过投资来赚取额外收入。他们也会像各国中央银行发行本国货币一样，发行额外的 Libra 来赚取铸币税。这些举动也将对央行采取货币政策带来了影响，Libra 并不由某个央行管控，如果人们更多持有 Libra 币而非该国法定货币，央行制定的货币政策对于国内经济的影响将会被削弱。

**Libra 面世之路注定一波三折。**截止目前为止，Libra 已经进行了三次听证会，仍面临全球尤其是欧美国家政府的巨大监管压力。监管的负面态度同时给参与其中的机构带来了巨大压力，MasterCard、visa、booking 等核心巨头退出 Libra 协会。在 10 月 23 号第三次国会听证会上，扎克伯格强调了 Libra 的战略意义：Libra 已经不是 Facebook 的 Libra，而是美国的 Libra，是美国建立数字货币全球支付体系的重要工具。另一方面，根据截止 10 月 24 日 Github 数据，Libra 自 2019 年 6 月代码开源以来，项目开发进度稳步推进，平均项目提交次数超过了比特币，是当前最活跃的公链之一。虽然 Libra 问世之路扑朔迷离，但是在区块链技术仍具有极高的探索价值。

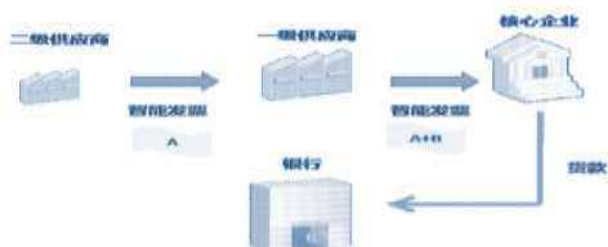
### 区块链方案低成本解决供应链金融价值传递问题——以易见股份为例

在供应链金融上，核心问题是应收账款的问题，商业银行更愿意向核心企业提供融资，因为商业银行信任核心企业的控货能力或是调节销售能力，而对于中小微企业的一级供应商等，银行通常不愿意提供授信，这就造成了这些企业的资金融通困难。

通过区块链技术，可以开发供应链金融的智能保理业务应用系统给供应链上的企业使用。首先二级供应商可以利用系统将开给一级供应商的记载着应收账款已转让给某银行的编码 A 的发票发布在区块链上，随后一级供应商再在此发票基础上添加其他必要编码，连同原转让信息变成编码 A+B，发布到区块链上。

依合同法第 79 条和第 80 条规定，此智能发票已达到债权转让法律通知的效果，核心企业当贷款到期时依法应直接将款项付给银行（如下图）。此外，银行也可以利用“智能保理”系统追溯每个节点的交易，勾画出可视性的交易全流程图，所以区块链技术为推广供应链金融“保理”业务到核心企业的二级以上的供应商提供良好的基础。

图 23：基于区块链智能保理应用系统



资料来源：《区块链在供应链金融的应用》，国信证券经济研究所整理

**基于区块链的供应链金融具体的交易流程。**首先是账户注册流程，基于区块链的供应链金融平台的参与方包括供应商用户、核心企业用户、系统平台用户、银行等。

之后各用户创建自己的账户，在链上创建对应的区块链用户，录入基础信息，并利用 RSA 加密规则产生相应的私钥和公钥，并在链上存储公钥的信息。之后供应商可以向核心企业、金融机构申请授信，核心企业、金融机构可以通过征信信息结合合同票据来判断是否予以授信并确定授信额度，平台便将授信金额，授信开始日，授信到期日生成数据写入链中。此过程需要平台私钥签名，供应商私钥签名、核心企业私钥签名、金融机构私钥签名。随后区块链会对平台业务数据进行链上处理，分配交易所属区块。

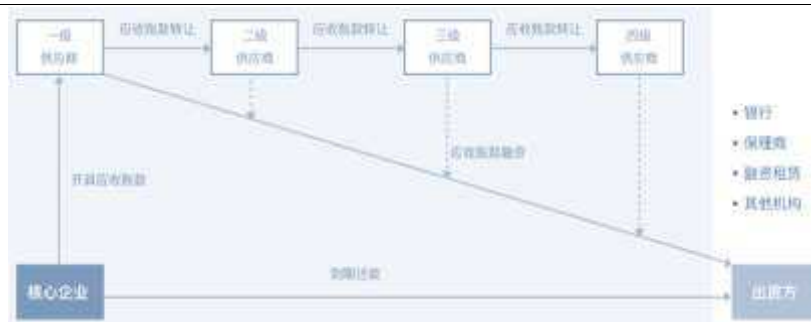
图 24：区块链在供应链金融中应用步骤



资料来源：供应链研究所，国信证券经济研究所整理

大型传统核心企业拥有自己的上游供应商和下游经销商链条，互联网、大数据、物联网等技术的运用将其信息流、数据流、物流和商流信息从线下逐步转移到线上管理。而区块链技术的加入，可以更好地对这些信息进行记录和追溯，使其信用价值逐步延伸并传递至链上长尾客户，帮助其获得更多融资机会。

图 25：区块链在供应链金融应用示意图



资料来源：趣链科技，国信证券经济研究所整理

一级供应商与核心企业产生应收账款后，一级供应商将应收账款记录到区块链中，生成对应的数字资产。当其与二级供应商(对应为一级供应商的经销商)产生赊销关系时，一级供应商可将与核心企业产生的数字化应收账款债权进行拆分，并在围绕核心企业的多级供应商和经销商之间进行流转。

图 26: 区块链+供应链金融业务逻辑



资料来源：电子发烧友，国信证券经济研究所整理

**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。

**举例而言，易见股份是一家将区块链技术应用用于供应链金融的企业。**易见供应链管理股份有限公司是一家现代供应链管理企业,专注供应链管理和供应链金融服务。公司的主要业务为供应链管理、商业保理业务以及基于公司“易见区块”平台提供的信息技术服务。其中供应链管理业务主要集中在控股子公司滇中供应链和全资子公司贵州供应链，业务模式是基于区域内具有强信用的核心企业，为其上游供应商和下游客户提供供应链管理及服务。商业保理业务主要集中在控股子公司滇中保理和霍尔果斯保理，其主要从事应收账款融资、应收账款管理及催收、金融信息咨询服务等业务。公司的信息技术服务主要集中在全资子公司易见天树和榕时代，通过提供“易见区块”平台服务，将公司供应链和保理服务向平台线上迁移。

图 27: 易见股份业务示例图





资料来源：公司官网，国信证券经济研究所整理

公司于 2018 年 9 月完成了“易见区块 2.0”平台升级，该平台采用了具有自主知识产权的“可信数据池”和业内领先的多链数据可追溯技术，实现了贸易、融资多链协同和跨链溯源，覆盖了供应链从贸易形成、融资到资产证券化的全过程。公司科研实力显著增强，积极与 IBM、Linux 基金会、清华大学经管学院、中国人民大学商学院、云南大学、西南林业大学等科研机构开展合作。15 年和 IBM 合作，以区块链技术切入供应链金融。目前区块链平台交易量已超过 70 亿。其中 ABS 业务上量很快，北交所的部分标准也是公司参与制定。

**易见区块业务爆发式增长。**在区块链业务板块，公司以全资子公司易见天树科技（北京）有限公司为核心进行区块链应用研发，以深圳市榕时代科技有限公司为区块链供应链金融签约和实施的主体，以霍尔果斯易见区块链商业保理有限公司为区块链商业保理业务主体，开展区块链供应链金融业务。**以上公司经营业绩在 2018 年已实现爆发式增长。**其中榕时代，2017 年仅实现收入 1.28 亿元，净利润 1.03 亿元，而 2018 年实现收入 2.60 亿元，净利润 2.07 亿元。霍尔果斯易见区块链商业保理，2017 年仅实现收入 955.78 万元，净利润 946.03 万元，而 2018 年实现收入 4.22 亿元，净利润 3.20 亿元。

图 28：易见区块作为供应链金融解决方案的核心优势



资料来源：公司官网，国信证券经济研究所整理

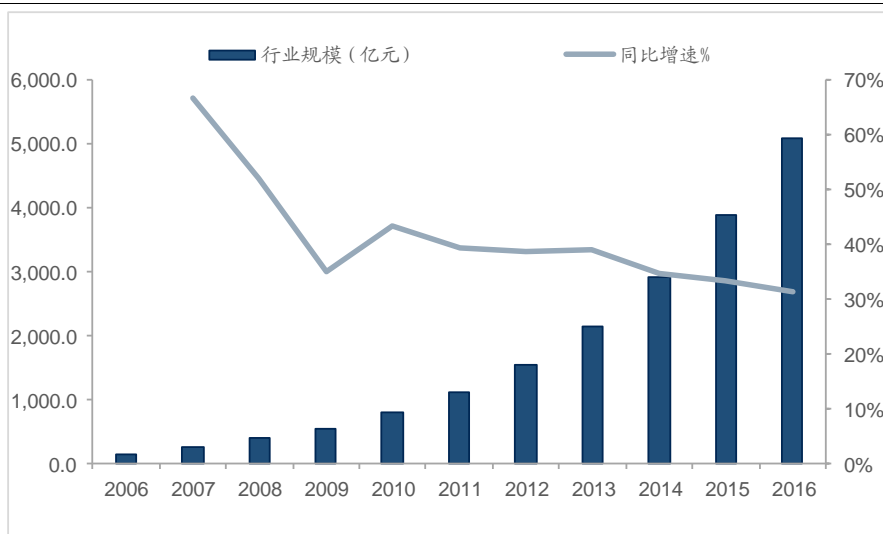
## 版权保护问题突出，区块链应用提供司法证据

中国网络版权产业规模突破 6000 亿元，并持续快速增长。国家版权局网络版权产业研究基地今天在京发布《中国网络版权产业发展报告（2018）》。



报告显示，当前我国网络版权产业继续保持快速增长趋势。根据测算，2017年中国网络版权产业的市场规模为6365亿元，较2016年增长27.2%。其中，中国网络版权产业用户付费规模为3184亿元，占比规模突破50%。2017年我国网络版权产业的体量已经成长为2013年的3倍。

图 29：2006-2016 年中国网络核心版权产业市场规模



资料来源：观研天下、国信证券经济研究所整理

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。

图 30：区块链版权登记流程图



资料来源：重庆小犀科技、国信证券经济研究所整理

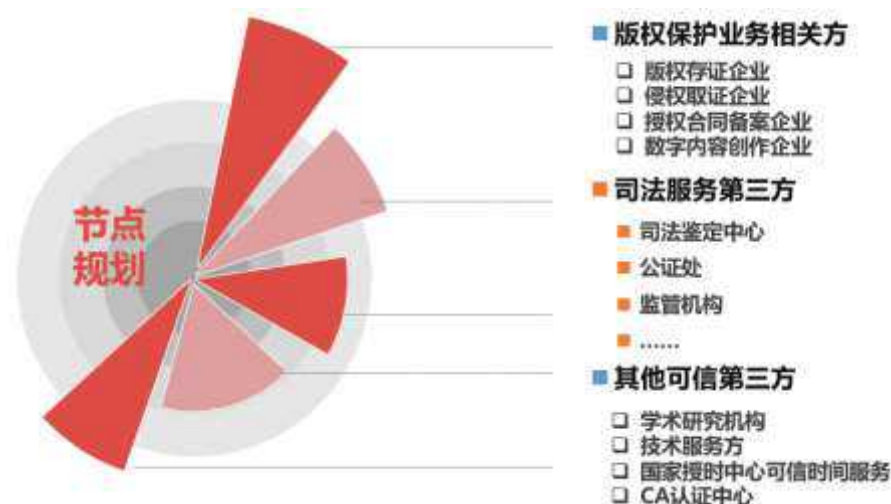
### 以安妮股份的版权区块为例:

安妮股份有限公司于 1998 年成立, 2008 年在深圳证券交易所挂牌上市, 以版权综合服务为主业, 是 A 股上市公司中的版权服务龙头企业。

公司提供基于区块链的版权存证服务(版权家), 已为百万作品提供了确权服务, 解决了内容创作者的痛点和难点。版权区块链首先通过对内容的数字摘要的计算和数字指纹提取上链, 保证了内容的完整性与原创性; 其次使用国家认可的数字证书机构颁发的证书提供数字签名, 结合国家授时中心可信时间实现数字作品的存在性证明、权属证明、授权证明和侵权证据固定。区块链系统参与者采用完全的实名数字身份认证机制, 并结合可信时间服务保证了作品的权属与存在时间。版权区块链做到将用户的整个创作过程完整记录, 从而发挥区块链技术在确权、授权与维权过程中的海量、快速、即时特性, 逐步实现“创作即确权、使用即授权、发现即维权”。

区块链核心解决各个链条参与者之间的信任问题, 规划节点包括版权保护业务相关方、司法服务第三方、其他可信第三方等。

图 31: 安妮股份版权区块链节点规划



资料来源: 公司公告、国信证券经济研究所整理

公司的版权区块链系统是基于 Hyperledger (超级账本) 与 FISCOBCOS 区块链平台开发, 具有版权确权、盗版监测、版权维权以及版权交易等功能的信息系统。系统通过核心层的存证合约、资产合约、交易记账合约, 以及服务层对智能合约的交互和调用, 能够为用户提供多种版权保护功能及接口服务。

版权区块链主要应用场景涉及确权、授权、维权三大领域, 面向自媒体作者、互联网编辑、网络漫画家等版权人, 提供整套的版权登记、交易、维权等服务。

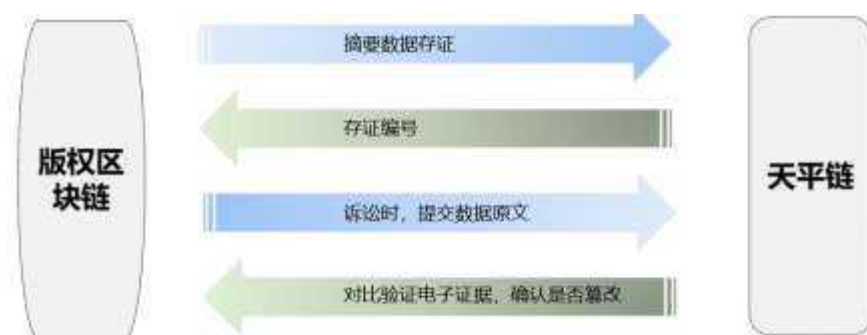
图 32: 安妮股份版权区块链应用具体场景

确权难:	侵权难:	维权难:
 <p><b>自媒体作者</b></p> <p>作品被侵权只用2小时</p> <p>互联网作品时效新鲜度约7天</p> <p>传统确权登记需10到30天</p> <p>登记花费300到1000元</p> <p><b>需求分析:</b> 权威、快速、低价的版权确权服务。</p>	 <p><b>互联网编辑</b></p> <p>在某图片渠道商购买图片用于文章配图</p> <p>收到了侵权律师函</p> <p>经调查渠道商所售的是盗版图片</p> <p>付出了高额赔偿费</p> <p><b>需求分析:</b> 权属清晰的、可追溯的、能够提供合法合同的授权服务。</p>	 <p><b>网络创作者</b></p> <p>发现原创被盗用到其他网站</p> <p>发现维权不及时、无详细数据</p> <p>传统公证取证时间长、费用高</p> <p>找不到合适的代理律师</p> <p><b>需求分析:</b> 及时发现、有效记录侵权行为、取证服务和维权代理。</p>

资料来源：公司公告、国信证券经济研究所整理

公司的版权区块链在维权取证过程中，实现为天平链提供版权比对信息，提供数据证据至天平链。“天平链”是由工信部安全中心、百度等国内领先区块链产业企业形成联盟共建的区块链电子证据平台，采用中国自研的百度超级链作为底层技术，具有支持混合架构，融合多链的技术优势。其联合鉴定中心、公证处等 17 个单位作为节点，接入包括百度图腾在内的 24 个应用，节点数和应用量均列国内司法行业第一。公司的版权区块链与天平链对接，凭借自身版权的记录信息，为天平链提供司法证据。

图 33：安妮股份版权区块链与天平链紧密对接



资料来源：公司公告、国信证券经济研究所整理

公司的版权家可信存证，帮助首个使用区块链证据进行判决的版权案件顺利结案。2014 年 5 月 10 日，AAA 公司发表一幅名为“快乐的年轻人玩手机和电脑”的图片。内容为四名男女青年，在观看手中的手机、笔记本电脑和平板电脑。2017 年 4 月 20 日，该图片被 BBBB 在未经版权人授权情况下私自使用，导致侵权案件的发生。AAA 公司通过版权家对进行作品的存证、侵权作品取证存证等一系列操作，将证据固定在版权链并同步到天平链，最终通过北京互联网法院法院电子诉讼平台进行立案，远程审理并胜诉。

图 34：首个使用区块链证据进行判决的版权案件

## 北京互联网法院 民事判决书

使用涉案图片的网页地址取证电子数据包。经国家版权局存证系统存证，自取证时间（2018年12月07日14:52:47）起已存在，且数据完整、未被篡改。后北京版权科技服务有限公司于2018年12月26日出具电子数据取证证书，确认注明公众账号“陈冠中（Chen Guangzhong）”的开办主体为“陈冠中”公司的网页地址取证电子数据包。经国家版权局存证系统存证，自取证时间（2018年12月26日14:52:38）起已存在，且数据完整、未被篡改。

北京版权科技服务有限公司为第三方存证平台。2019年1月1日注册登录北京互联网法院电子存证系统后，任何存证用户在国家版权科技服务有限公司进行存证的同时，北京互联网法院电子存证系统均会对其存证数据的哈希值进行同步存储。本案中，原告公司于2019年2月6日再次通过北京版权科技服务有限公司存证系统上传证据，并于3月11日通过北京互联网法院电子存证平台向本庭提交该证据。在提交证据时，电子存证平台同步生成该证据的哈希值，并存储该哈希值与原告存证平台提供的存证时产生的哈希值进行对比，得出区块链存证验证成功的验证结果，并司法留痕。据此可以确定相关网页在存证后未经篡改。被告亦对电子存证的验证结果没有异议。被告虽辩称其使用原告公司的图片属于转载，提供了其他员工与他人的微信聊天记录，被告对此证据的真实性亦不持异议。综上，本院对以上证据的真实性、合法性及关联性均予以认定。根据以上证据，

《2019》京0491民初724号

一、被告于本判决生效之日起十日内，赔偿原告（原告）经济损失2000元及合理开支500元，以上合计2500元；

二、驳回原告（原告）其他诉讼请求。如果被告未按本判决指定的期间履行给付金钱义务，应当依照《中华人民共和国民事诉讼法》第二百五十三条之规定，加倍支付迟延履行期间的债务利息。

案件受理费25元，由被告（被告）负担。原告（原告）负担。

如不服本判决，可在判决书送达之日起十五日内，向本院递交上诉状，并按对方当事人的人数提出副本，上诉于北京知识产权法院。如上诉期满七日内未交上诉案件受理费，按自动撤回上诉处理。



本卷与正本核对无异

资料来源：公司公告、国信证券经济研究所整理

## 国际结算与跨境支付中高昂的费用问题，有望使用区块链解决

由于身份验证与监管原因，跨境汇款的费用较高。据世界银行数据：世界银行2016年数据显示(Remittance Prices Worldwide, Issue n. 19, September 2016)，G20国家的平均汇入成本为7.56%。银行渠道的SWIFT跨境汇款费用按照阶段可以分为：汇出时：电报费、手续费；中间行费用；入账时的入账费；此外还有查询费用、转报费用等，环节复杂，费用高昂。而区块链建立去信任、去中心化交易体系，有望显著缩减费用。

图 35：传统的跨境转账涉及众多手续费环节



资料来源：搜狐科技，国信证券经济研究所整理

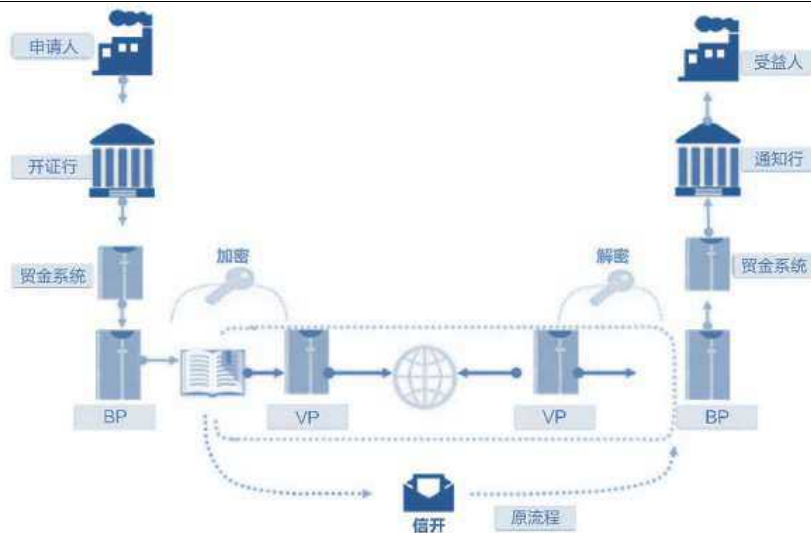
**区块链业务流程：**以信用证业务举例：由开证行发起生成第一区块，开证人将信用证信息转化为数字资产存储于智能合约中，键入此笔交易的信用证主链。生成后向申请人、受益人“广播”，受益人以“私钥”打开该区块，获取信用证信息。以此来开立和通知信用证。在第一区块之后，由受益人创建第二区块，并嵌入应有受益人提交的单据，如发票、汇票等。保险人、船公司进入第二区块，通过分布式记账的方式记录各自领域的交易信息，分别嵌入保险单据、运输单据等，融入到此笔交易的主链中。受益人发货后，通过主链可以实时跟踪货物动态，直至收到货款。之后开证行凭私钥打开第二区块，单据审核无误后，



将私钥共享给申请人。等到信用证到期日，开证人将申请人账户上的区块链数字货币转移至受益人账户。

**物理架构：**系统由三级构成：参与机构的业务系统、区块链前置 BP、区块链节点 VP。业务主要流程如下：开证行 BP 节点受理电开信用证数据；BP 节点进行交易加密；通过 VP 节点写入区块链；通知行 VP 节点读取区块链；通知行 BP 节点解密；无误后送通知行资金系统；通知受益人，受益人确认后发货开单。

图 36：基于区块链的信用证系统物理架构

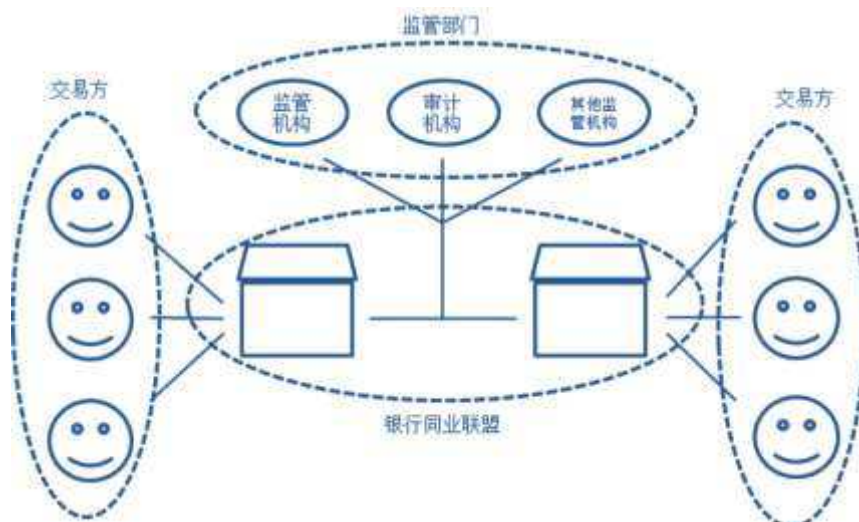


资料来源：金融咨询网，国信证券经济研究所整理

**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。

**举例而言：**2016 年 12 月，俄罗斯阿尔法银行 Alfa- Bank 与 PJSC 西伯利亚航空公司通过以太坊（Ethereum）区块链智能合约（Smart Contract）进行了信用证交易。在交易中，区块链智能合约记录了该银行在区块链上执行的信用证操作，区块链智能合约包括了以下信息的哈希值（Hash values）：信用证的价值、信用证开具和关闭的日期等核心信息。申请人使用阿尔法银行的在线系统申请信用证开立，卖方（受益人）在区块链系统中提交电子单据。信用证开立后，阿尔法银行从客户账户中扣除一部分特殊资金（等值于信用证金额），待受益人提交相符单据后，将这些资金转移至卖方（受益人）账户中。

图 37：银行国际结算业务体系各交易主体结构简图



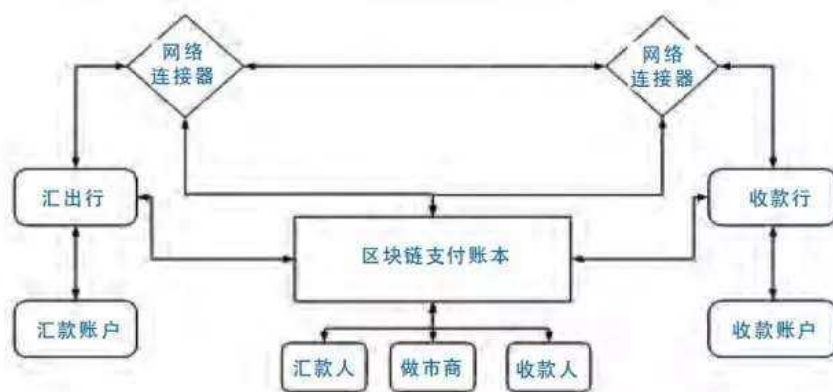
资料来源：《基于区块链技术的银行国际结算业务经营创新》，国信证券经济研究所整理

区块链技术也越来越多地应用于了银行国际结算领域如国际保理，托收等业务，区块链的使用使得交易更加安全，重建了信任机制，提供了匿名性，并且减少了纸质单据在进出口商之间的流通，去除了人工审核的成本，成为国际结算中一个重要的创新趋势。

**区块链技术在跨境支付中也获得了应用。**现有的跨境支付普遍采用 SWIFT 网络，而区块链的使用，有着周期长，手续费用高的缺点。

**业务逻辑：**接入区块链技术后，通过公私钥技术，保证数据的可靠性，再通过加密技术和去中心，达到数据不可篡改的目的，最后，通过 P2P 技术，实现点对点的结算；去除了传统中心转发，提高了效率，降低了成本。首先通过电子档案方式建立付款人与银行/转账服务商之间的信任，通过智能合约记录收款人和付款人之间转账行为的权利义务关系。之后通过智能合约传输交易信息如收付款身份，汇率，金额等，实现实时转账。监管机构可实时进行交易监控，通过智能合约接受 AML 预警和提示。之后通过智能合约将资金存入收款人账户，由收款行执行相关流程后收款人提取。交易后得益于分布式数据记账功能，相关交易记录仍保存，监管机构可后续审查。

图 38：区块链跨境支付架构图



资料来源：银通智略，国信证券经济研究所整理

**技术优势：**

1.降低跨境支付风险。进出口商资金支付，出口商发货信息真实性是传统电汇支付的最大风险。进口商对于电汇中间支付环节缺乏足够信息，无法干预资金转移，同时难以了解出口商的发货消息，电汇依照商业信用为基础进行交易，存在贸易风险。区块链技术的跨境支付，可以将进口商，出口商，金融机构作为节点链接起来，一起检验维护核对交易信息。进口商在通过区块链支付之后，如果未能收到真实有效的出口商发货信息，便可在一致性校验环节否认收到发货信息，拒绝付款，出口商便不能收到汇款。因此，通过区块链支付，所有交易相关方共同维护交易记录，参与验证交易信息，可以降低国际贸易中原本基于商业信用的交易风险。

2、提高跨境支付效率。传统电汇由银行主导交易，银行间支付由中央交易方完成，中间交易方拥有本地数据库，记录账户余额和流水，是交易中的权威账本。在这种具有中间参与方的交易中，必然经过两个复杂的业务处理：第一，所有参与支付的银行，必须对交易信息进行对账，并将所有交易信息同步到中间结算方。第二，中央交易方要在抵消不同账户的借贷后，才执行最终的支付。因此，在传统跨境支付中，需要非常复杂的交易处理。采用区块链支付的解决方案，由于区块链网络中所有参与节点共同维护验证信息，保证了信息的一致性，因此，在区块链支付中无需复杂的信息同步和对账，大大提高跨境支付的效率。

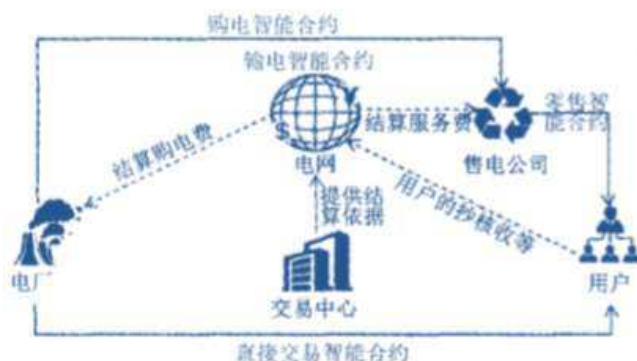
3、节省银行业务资源。在传统跨境支付中，银行之间的汇款每个银行都为关联银行建立支付网络，开设单独的准备金账户，进行借记贷记，以保证汇款的安全性，最小化对手风险。而这就需要大量的准备金用于跨境支付。利用区块链技术可以大大降低准备金，从而节省银行业务资源

举例而言：2018年6月，蚂蚁金服在香港推出了全球首个基于区块链技术的跨境汇款服务。AlipayHK（港版支付宝）的用户可通过手机向菲律宾钱包 Gcash 汇款，因为是基于区块链技术，所以能够实时到账，降低了汇款成本，同时能够提升交易过程的透明度，在港工作 22 年的菲律宾人 Grace 使用蚂蚁金服的新功能，仅用时 3 秒就完成了汇款，这在以前需要 10 分钟到几天的时间。

### 区块链有望解决电力产业链中发电、传输、交易、用户各端的互信问题

在电力市场中，区块链也将被广泛应用。在区块链中，电厂作为生产者在产电后，将电力虚拟化为一种数字资产，向全网广播，登记发行到区块链上，之后电能即可进行交易，用户和电力公司实时交互，在区块链智能合约的支持下，查看交易信息，电力的流转和快捷支付能够高效的运转，完成购电。电费的收缴可以采用区块链智能合约将每一个交易的输入分别输入到不同的对象中，利用交易介质进行支付结算。

图 39：基于智能合约的电力市场交易模型

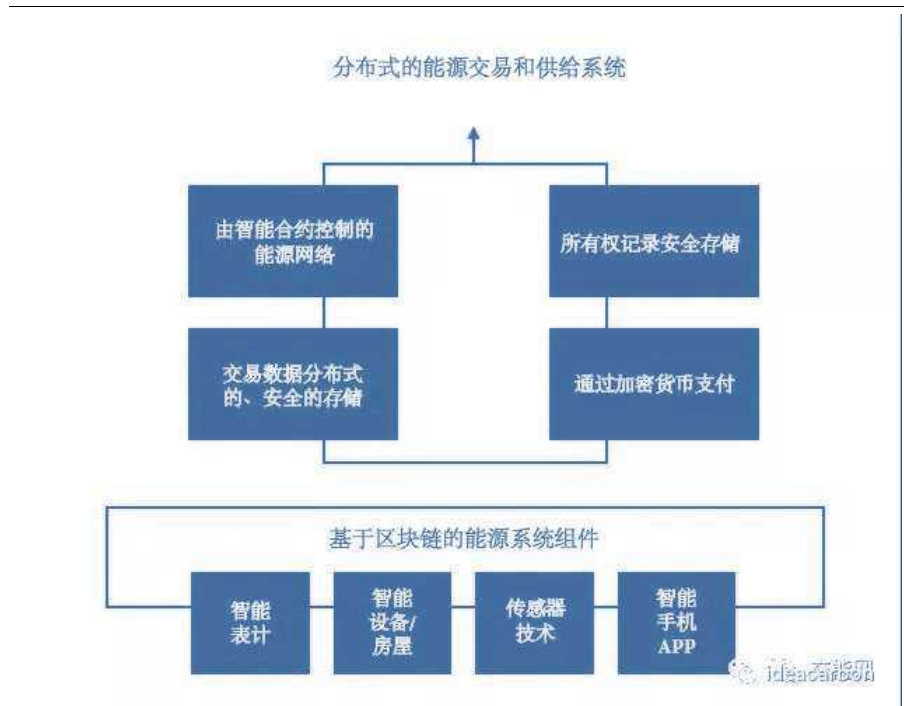


资料来源：《基于区块链的电力市场交易结算智能合约》，国信证券经济研究所整理

在区块链模式下，电力生产者，售电部门和消费者可以实现“直连”。三者之间

的关系通过所谓的“智能合同”实现约束，“智能合同”本质上就是一种特殊的计算机协议，用以约束能源产销各方。运用智能电表，可以预测计算每位消费者对电力的需求，电厂也同样可以计算出预期的电量供给。网络中心即可对消费的需求预期以及电厂供给预期进行匹配。分布式电力行业或许将因为这一运营模式产生革命性变化。原本无法动态交易的家庭分布式设备在未来都有机会接入到一个大的网络中。总之，将区块链应用于电力行业上可以提供互信，提升网络安全，提高电力系统生态的效率。

图 40：基于区块链的能源系统结构



资料来源：交能网，国信证券经济研究所整理

**技术优势：**将区块链技术用到电力分配当中将会在很大程度上解决了电力分配不均匀的问题或者是偷电的问题。将电网区块链化，那么电业管理的人员就可以随时监管用电情况，而且会很容易看出来是否有人的用电量与购买量是否相符，而且因为区块链的存在，用电数据也无法被重新篡改，这样的话，就能最大程度地保证用电情况的真实性。同时分布式能源及存储设备凭借其灵活、清洁的特点，在提高局部供电可靠性、降低输电损耗、增加能源利用面具有很好的应用前景。

**举例而言：**在纽约，LO3 Energy 和 ConsenSys 合作在纽约布鲁克林区实现了一个点对点交易、自动化执行、无第三方中介的能源交易平台，实现了 10 个住户之间的能源交易和共享。用户在家门口安装智能电表，安装区块链软件成链，之后用户在区块链节点上发布相应智能合约，基于合约规则，实现能源交易和能源供给。

除此之外区块链可以为电动车辆（EV）充电提供协调服务。地区建立区块链微电网，每个电站的电价可以由电网和住宅电力供应商共同建立。司机可以使用区块链钱包，通过区块链账本，按照智能合约的规定安全地即时付款。这种方式将让电动汽车充电变得更加便捷，有助于推广电动汽车的使用。

### 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。

**应用流程：**不同机构所搜集的用户数据先临时缓存到自身的后台数据库中，并根据用户特有的身份信息帮助其创建独有的数字身份和相应的公私密匙对。之后本地节点将所有用户身份信息抽离出来，敏感数据打包加密存储至身份管理池中，脱敏数据分往不同的服务器。此时没有机器可以提取基本信息，但是节点仍然可以共同计算数据的授权功能，而身份管理池由系统随机选定可信任节点来确保用户身份数据的合法写入及不同账号数据关联的建立。这样一来，只要有药企、保险商为用户数据付费，即可借助智能合约按各方数据贡献比进行实时分红。

药企在后台管理系统提交自身要售卖的药品、服务，向系统发出分析请求。系统收到后抽取其相应客户受众可能具备的病理特征，再据此向目标客户群（系统初步判断）发出授权请求，用户同意且药企支付费用后，系统将目标用户病理特征与授权群体中的病理特征（已脱敏）进行比对，并将对比结果及相似度反馈至药企。药企查阅后可选择相似度达 60% 以上的筛选条件作为门槛，向目标客户推送定制化服务。

保险商在后台管理系统提交自身要售卖的服务，并向用户群体发出授权请求。用户同意且保险商支付费用后，系统评估授权群体中患有某种疾病风险的概率，并将相关结果反馈至保险商，其查阅后可根据用户群体患有某种疾病的概率进行智能定价，并将不同的定制化服务推送至用户。

图 41：医疗行业区块链应用示意图



资料来源：创空网，国信证券经济研究所整理

**应用优势：**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。

去中心化的交易。从数据的获取、扩展和安全方面来看，基于区块链的分布式账本（DLT）这一基础设施，要比现有的中心化系统更强。而且，去中心化的系统也可以简化成本结构，减少交易时长，免除不必要的中间商和管理费用，从而性价比也更高。

图 42：医疗领域应用区块链示例



资料来源：Deloitte, 《Blockchain: Opportunity for Health Care》, 国信证券经济研究所整理

#### 举例而言：

1、电子健康病历（EHR）医疗方面，区块链最主要的应用是对个人医疗记录的保存，可以理解为区块链上的电子病历。如果把病历想象成一个账本，原本它是掌握在各个医院手上的，患者自己并不掌握，所以病人就没有办法获得自己的医疗记录和历史情况，这对患者就医会造成很大的困扰，因为医生无法详尽了解到你的病史记录。但现在如果可以用区块链技术来进行保存，就有了个人医疗的历史数据，有历史数据可供看病或对自己的健康做规划使用，这个数据真正的掌握者将是患者自己，而不是某个医院或第三方机构。

2、DNA 钱包基因和医疗数据能够运用区块链技术进行安全存储并且通过使用私人密钥来获得，这将形成一个 DNA 钱包。这使得医疗健康服务商能够安全地分享和统计病人数据，帮助药企更有效率地研发药物。而这种模式也正在逐步建立起来。

3、比特币支付区块链技术的发展促进了比特币支付，给予病人进行保险支付更多的选择。虽然这也依赖于比特币在市场上的发展状况，但提供这一方式的保险公司相对于竞争对手来说也有着更大的优势。对于健康医疗保险公司而言，区块链作为金融服务的一个部分正在被建立。

4、药品防伪与编码防伪，对于运用区块链技术防伪的药品而言，在药品包装盒表面有一个可以被刮去的面，底下是一个特别的验证标签，这与区块链相互对照来确保药品的合法性。

DHT（Deep Health Chain）于 2018 年 2 月 28 日在新加坡上线，是一个基于区块链的医疗健康服务平台，构建了一个自治的生态体系。患者在体系中是主要的参与者，患者可以将自己的医疗数据上传到 DHC 链中，通过智能合约设置一定的权限，有效地保障了用户自己的数据隐私。DHC 整个生态目前拥有 30 多家三甲医院和数百家医疗机构的医疗数据，其所创建的生态市场可应用于个人健康报告、完整的药品供应链、医药临床试验和人口健康研究。

表 9：机构医疗信息安全与隐私保护区块链应用项目列表

项目/案例	涉及内容	企业
-------	------	----

爱沙尼亚 e-health	医疗数据健康	Guardtime
FDA 与 IBM 联合区块链研究	医疗数据健康	IBM Watson Health
常州市医疗区块链项目试点	医疗数据健康	阿里健康
河北廊坊的区域卫生信息平台	医疗数据健康	云巢智联
趣医网	医疗数据健康	趣医网
澳大利亚卫生部	医疗数据健康	Agile Digital
Recovery coin	医疗数据健康	Consensus
阿联酋 Du 和 NMC Healthcare 合作	医疗数据健康	Guardtime

资料来源:健康界, 国信证券经济研究所整理

## 计算机行业上市公司纷纷布局, 重点关注金融 IT 领域龙头公司

**第一批区块链项目完成正式政府备案, 部分上市公司得到入选。**2019 年 3 月 30 日, 国家互联网信息办公室正式发布第一批境内 197 个区块链信息服务备案编号, 《区块链信息服务管理规定》于今年一季度正式实施。此次公布的第一批名单中包括百度、京东、腾讯、爱奇艺等互联网上市公司, 也有金融或其他实体经济领域公司包括陆金所、浙商银行、浪潮集团、海尔集团、中国平安、众安保险、微众银行、顺丰、华大基因、好未来教育等公司或旗下企业获首批区块链备案编号。上市公司方面, **易见股份全资子公司易见天树和榕时代科技; 安妮股份旗下版权家科技; 晨鑫科技旗下竞斗云以及华大基因也进入首批名单。**此次备案是监管部门依法对区块链行业进行规范的行政措施, 同时体现了监管对区块链行业发展的鼓励, 区块链行业逐步进入规范轨道。

区块链提供安全与信任的技术架构, 当下重点在金融领域的应用需求较为迫切, 建议关注布局区块链的上市公司: **恒生电子、金证股份、易见股份、同花顺、航天信息等。**

**恒生电子:** 金链盟 (金融区块链联盟) 成员之一。公司牵头运营的 FTCU 链已经实现了电子合同签署、电子邮件存证等基础性应用; 面向香港场外业务开发的香港青链, 将原来场外业务从繁琐的手工过程中解放出来, 促进了效率提升; 基于区块链技术不可篡改等特性开发辅助供应链融资、不良资产等应用场景。

**金证股份:** 金链盟 (金融区块链联盟) 成员之一。据上海证券报消息, 金证股份的区块链技术已完成在证券局部业务上的验证, 其性能实现跨越式提升。

**易见股份:** 全资子公司易见天树和榕时代科技入选国家互联网信息办公室第一批境内区块链信息服务备案名单。在区块链业务板块, 公司以全资子公司易见天树科技 (北京) 有限公司为核心进行区块链应用研发, 以深圳市榕时代科技有限公司为区块链供应链金融签约和实施的主体, 以霍尔果斯易见区块链商业保理有限公司为区块链商业保理业务主体, 开展区块链供应链金融业务。**以上公司经营业绩在 2018 年已实现爆发式增长。**其中榕时代, 2017 年仅实现收入 1.28 亿元, 净利润 1.03 亿元, 而 2018 年实现收入 2.60 亿元, 净利润 2.07 亿元。霍尔果斯易见区块链商业保理, 2017 年仅实现收入 955.78 万元, 净利润 946.03 万元, 而 2018 年实现收入 4.22 亿元, 净利润 3.20 亿元。

**同花顺:** 公司已储备一定的区块链相关技术, 并积极探索区块链相关技术在互

联网金融信息服务领域的应用。

**航天信息：**公司在 2016 年就着手研究研究区块链技术，开发了自主知识产权的面向企业级应用的基础开发平台——区块链技术开发平台，已经成功应用于电子发票等领域，该平台目前已在湖北、山东、北京、内蒙和宁夏 5 个地区开展试点工作，进展良好。

**表 10：计算机行业上市公司区块链布局梳理**

公司	项目名称	项目介绍	与区块链结合方向
恒生电子	FTCU 链	电子合同签署、电子邮件存证等	金融交易
金证股份	证券业务区块链	完成在证券局业务上的验证	金融交易
华宇软件	法院司法链平台	与蚂蚁区块链合作,现已为法院或当事人提供办案全流程规范化监管、网络著作权存证云等五项链上服务	司法服务
航天信息	区块链技术开发平台	已经成功应用于电子发票等领域,该平台目前已在湖北、山东、北京、内蒙和宁夏 5 个地区开展试点工作	电子发票
易见股份	易见区块	供应链信用体系	供应链金融
宇信科技	区块链+金融	与质数链网就 ABS(资产证券化)、供应链金融等领域开展全面深入的合作	供应链金融、ABS
安妮股份	版权家	版权确权、授权、监测、维权、交易	版权保护
二三四五	2345 星球联盟计划	云存储、积分系统	数据保护
三六零	共享云	基于区块链的安全共享云平台,通过 360 共享云产品分析闲置的带宽资源、计算资源、存储空间	数据保护
润和软件	信用证	区块链保函、区块链信用证、区块链保理等	金融交易
赢时胜	泛资管阳光链	在日常划款指令中运用区块链,实现管理人和托管人业务与区块链基础业务无缝对接	金融交易
四方精创	MinimumViable Product	实现保险政策数据实时共享	保险

资料来源：各公司官网、国信证券经济研究所整理



## 国信证券投资评级

类别	级别	定义
股票 投资评级	买入	预计 6 个月内，股价表现优于市场指数 20%以上
	增持	预计 6 个月内，股价表现优于市场指数 10%-20%之间
	中性	预计 6 个月内，股价表现介于市场指数 $\pm 10\%$ 之间
	卖出	预计 6 个月内，股价表现弱于市场指数 10%以上
行业 投资评级	超配	预计 6 个月内，行业指数表现优于市场指数 10%以上
	中性	预计 6 个月内，行业指数表现介于市场指数 $\pm 10\%$ 之间
	低配	预计 6 个月内，行业指数表现弱于市场指数 10%以上

## 分析师承诺

作者保证报告所采用的数据均来自合规渠道，分析逻辑基于本人的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

## 风险提示

本报告版权归国信证券股份有限公司（以下简称“我公司”）所有，仅供我公司客户使用。未经书面许可任何机构和个人不得以任何形式使用、复制或传播。任何有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以我公司向客户发布的本报告完整版本为准。本报告基于已公开的资料或信息撰写，但我公司不保证该资料及信息的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映我公司于本报告公开发布当日的判断，在不同时期，我公司可能撰写并发布与本报告所载资料、建议及推测不一致的报告。我公司或关联机构可能会持有本报告中所提到的公司所发行的证券头寸并进行交易，还可能为这些公司提供或争取提供投资银行业务服务。我公司不保证本报告所含信息及资料处于最新状态；我公司将随时补充、更新和修订有关信息及资料，但不保证及时公开发布。

本报告仅供参考之用，不构成出售或购买证券或其他投资标的的要约或邀请。在任何情况下，本报告中的信息和意见均不构成对任何个人的投资建议。任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。投资者应结合自己的投资目标和财务状况自行判断是否采用本报告所载内容和信息并自行承担风险，我公司及雇员对投资者使用本报告及其内容而造成的一切后果不承担任何法律责任。

## 证券投资咨询业务的说明

本公司具备中国证监会核准的证券投资咨询业务资格。证券投资咨询业务是指取得监管部门颁发的相关资格的机构及其咨询人员为证券投资者或客户提供证券投资的相关信息、分析、预测或建议，并直接或间接收取服务费用的活动。

证券研究报告是证券投资咨询业务的一种基本形式，指证券公司、证券投资咨询机构对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向客户发布的行为。

## 国信证券经济研究所

.....

### 深圳

深圳市罗湖区红岭中路 1012 号国信证券大厦 18 层

邮编: 518001 总机: 0755-82130833

### 上海

上海浦东民生路 1199 弄证大五道口广场 1 号楼 12 楼

邮编: 200135

### 北京

北京西城区金融大街兴盛街 6 号国信证券 9 层

邮编: 100032