2016 年 4 月 17 日

计算机行业

光大证券 EVERBRIGHT SECURITIES

区块链：去中心化利器，重塑信用机制

行业深度

◆区块链是一个去中心化的分布式记账数据库

记账方式随着商业社会的发展不断进化，未来的世界是去中心化的。区块链通过规则和算法建立了一个去中心化、去信任、集体维护且可靠的分布式记账的数据库，重塑了商业活动中的信用机制，将给货币、支付、股票债券交易、政府、艺术品等领域带来颠覆性的影响。根据世界经济论坛调查报告预测，到 2025 年全球 GDP 中有 10%的相关信息将用区块链技术保存。

◆共识机制、分布式网络、非对称加密和智能合约是区块链的核心

共识机制调配记账节点的任务负载，维持区块链账本的运转与更新。分布式网络使得每个记账节点实现了去中心化的沟通，数据得以灵活地传播与验证。非对称加密用来验证交易的真实性，保障了每个人对财产的所有权。智能合约赋予了区块链灵活的可编程特性，是货币、金融、社会等应用领域得以可编程的重要基础。

◆生态平台和高粘性的场景应用最具价值

技术层是区块链账本的技术支撑，包括数据层、网络层、共识层、激励层、合约层五个层次；应用层是连接业务场景和区块链账本的桥梁，主要分为软件应用和硬件应用两类。二者共同构成区块链的系统框架，且由此延伸出三类商业模式：生态平台、垂直应用和第三方技术提供方。我们认为形成生态的平台和具有高粘性的场景应用将具有巨大价值，而第三方技术提供方通过技术支持和服务等方式也能获取一定的收入。

◆发展逐步升级，应用百花齐放

区块链的应用层划分为 1.0、2.0 和 3.0 三个阶段：1.0 是可编程货币，是与转账、汇款和数字化支付相关的密码学货币应用；2.0 是可编程金融，是经济、市场和金融领域的区块链应用，例如股票、债券、期货、贷款、抵押、产权、智能财产和智能合约；3.0 是可编程社会，是超越货币、金融和市场的应用，特别是在政府、健康、科学、文化和艺术领域的应用。当前处于 1.0 成熟，2.0 拓展，3.0 探索的阶段，随着技术的进一步成熟与更大范围的普及，应用领域将会百花齐放。

◆推荐对区块链技术应用积极性最高的金融领域潜在受益标的

结合国内区块链领域的发展现状，我们认为将区块链技术应用到垂直领域未来将大放异彩，尤其是目前对区块链技术应用积极性最高的金融领域，潜在的实践者包括金融 IT 公司和第三方支付企业，重点推荐海立美达、广电运通和御银股份。建议关注恒生电子、赢时胜、飞天诚信。

◆风险分析：

技术发展不顺利，行业应用进展不顺利。

证券代码	公司名称	股价	EPS			PE			投资评级
			15A	16E	17E	15A	16E	17E	
002537	海立美达	28.17	0.11	0.47	0.63	256.1	59.9	44.7	买入
002152	广电运通	26.90	0.83	0.97	1.11	32.4	27.7	24.2	增持
002177	御银股份	8.78	0.09	0.17	0.21	96.2	50.7	42.5	增持

买入（维持）

分析师

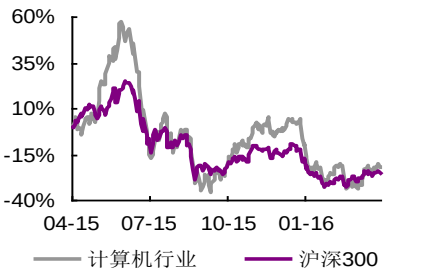
姜国平 (执业证书编号：S0930514080007)
021-22169167
jianggp@ebscn.com

薛亮 (执业证书编号：S0930515050004)
021-22167311
xueliang@ebscn.com

联系人

卫书根
021-22167336
weishugen@ebscn.com

行业与上证指数对比图



目 录

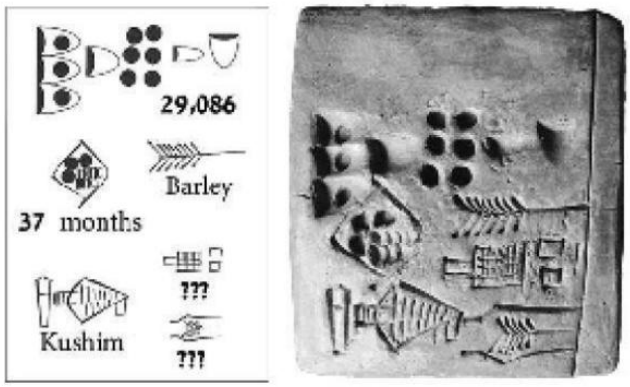
图表目录

1、人类记账史的进化

人类社会为了克服人脑的问题做了记账的体系。当农业社会出现私有制和所有权概念的时候，如何测量、税务、贸易就成了需要解决的问题。而人脑具有自我欺骗的特征，当超过150人后账目就很难管理，因此需要借助数学工具，进而演变成应用到金融领域的金融技术。金融技术起源于如何证明权利的真实性，其基础是记录资产的合约，体现了记录对象的物质属性和技术属性。因此，人类社会为了克服人脑的问题发明了记账的体系，通过把相关协议和合约记录出来，从而实现了金融追索权物质化。

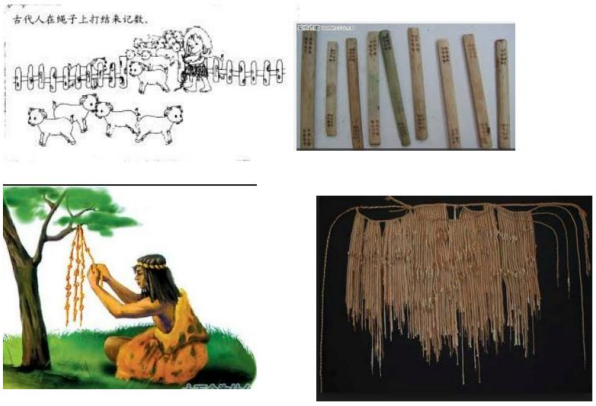
区块链是互联网时代的记账方式。记账的历史经历了一个漫长的发展过程，从最初的包括结绳计数、算筹、符木等的符号记录，到促进资本主义发展的复式记账法，记账方式的发展与经济活动的发展相互促进。而区块链系统则是互联网时代的一种记账方式，其以数学算法作为背书，在一个公开透明的数学算法之上建立了一个能够让所有不同政治文化背景的人群达成共识的信用机制，所涉及的也是记账、对账、分账等科目，而凡是和经济活动相关的信息都属于记账的范畴，因此其具有广泛的应用领域。

图1：苏美尔人用泥板计数



资料来源：互联网

图2：结绳计数、算筹计数



资料来源：互联网

2、记账方式的颠覆式创新

2.1、区块链：集体参与的去中心化的分布式数据库

未来的世界是去中心化的。信息的不对称使得中心化的结构在现实生活中比比皆是：我们的汇款需要通过银行中转，网上交易需要支付机构担保，买卖房产需要通过房产中介等等。中介机构的存在一定程度上解决了交易双方的信任问题，但同时也带来了抬升交易成本、降低交易效率以及中介本身的道德风险等问题。互联网的出现大大的降低了信息不对称的程度，在网络世界中的低金钱敏感度的领域，去中心化的组织已经初见雏形。比如众筹，一个独立的个体参与一起众筹是基于自身对该项目的认知，而不依赖于众筹平台本身的大小，实际上众筹平台也并不为众筹项目的价值提供担保。

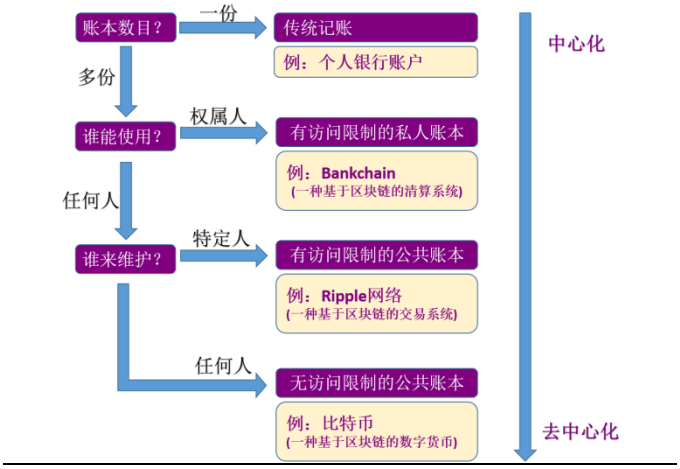
区块是交易系统中每一个时间段所有交易的电子化记录。创世块生成之后，当一个节点向全网所有节点广播交易需求时，所有愿意参与的节点都可以响应交易。同时通过一定的共识机制选择部分节点参与该段时间内的交易记录，当交易记录被全网多数节点验证通过便形成记录该段时间交易的区块。

区块的结构一般包括块头和块身两部分，其中块头是该区块与前一个区块的索引以及该区块的相关情况，块身则记录了该笔交易的信息。只要一个交易系统没有关闭，理论上区块会随着新交易的不断达成而不断产生，并不断的更新保存到每一个系统内的节点。

链的基础是时间戳，保证了区块链系统的可溯源。交易有先后，对应的区块的生成也有先后，区块按照时间先后顺序连接形成区块链。由于每一个区块上记录的交易信息均存在于每一个系统内节点且对于全网是可见的，因此所有系统内节点参与的交易记录以及实时的留存价值都是可查询的，这就解决了参与交易的门槛和节点真实性难题，解决了交易过程中的信任问题并实现了区块链系统本身的可溯源。无疑，可溯源性消除了参与交易方的道德风险，避免了无效交易和虚假交易的发生。此外，透明的交易信息绑定的是交易节点，而节点背后的个人则被隐藏，从而解决了隐私的问题。

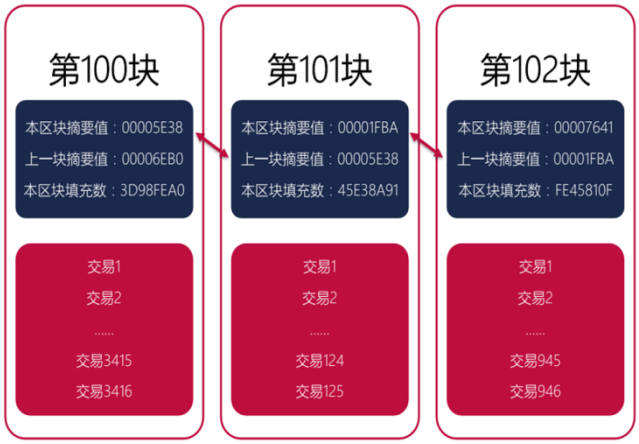
区块链的本质是一种分布式记账的数据库。在基于同一个交易协议的基础上，当一笔交易发起时，该交易系统内的所有节点都可以参与交易的响应。将一段时间内的所有交易信息记录下来并形成一个区块，按时间前后相连就形成区块链。因此，区块(完整历史)与链(完整验证)相加便形成了区块链(可追溯完整历史)，其存储了该交易系统从第一笔交易发起至今的所有历史数据，并为每一笔数据提供检索和查找功能，能够逐笔验证。

图 3：记账方式分类



资料来源：《Distributed Ledger Technology :beyond blockchain》

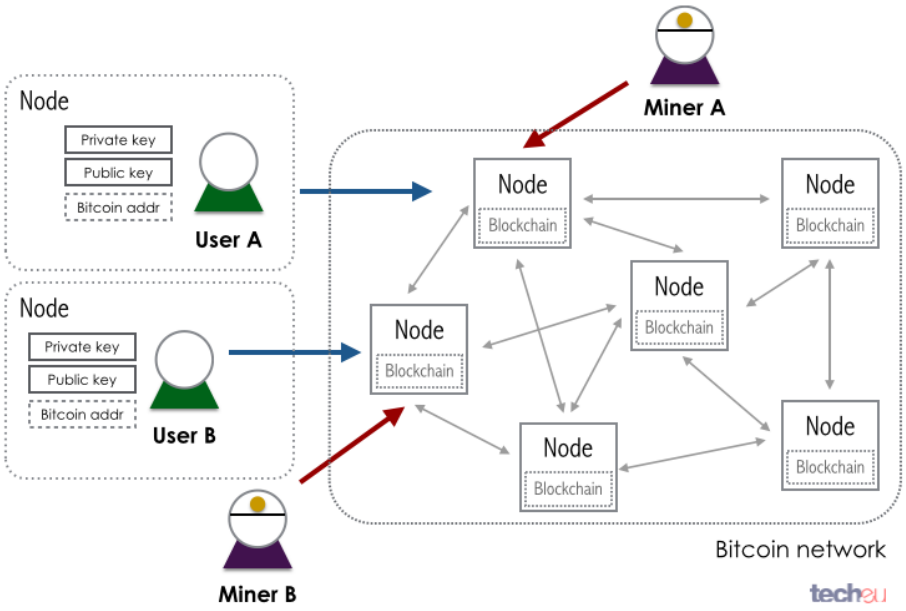
图 4：区块链组织结构示意图



资料来源：《小蚁白皮书》

以比特币为例，可以把区块链想象成一个比特币的公共账本。第一，这个账本存放在互联网的各个比特币节点上，每个节点都有一份完整的备份。第二，这个账本记录着自比特币诞生以来的所有比特币转账交易。第三，这个账本是分区块存储的，每一块包含一部分交易记录。每一个区块都会记录着前一区块的 id，形成一个链状结构，因而称为区块链。第四，当要发起一笔比特币交易的时候只需把交易信息广播到网络中，矿工把交易信息记录成一个新的区块连到区块链上，交易就完成了。

图 5：比特币网络



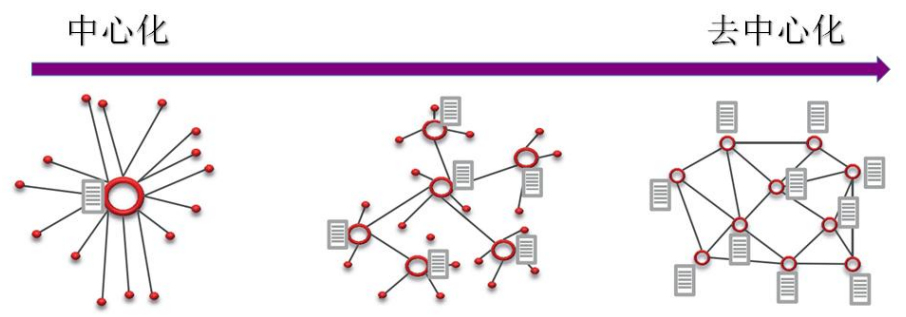
资料来源：tech.eu

共识机制、分布式网络、非对称加密和智能合约是区块链的核心。共识机制调配记账节点的任务负载，维持区块链账本的运转与更新。分布式网络使得每个记账节点实现了去中心化的沟通，数据得以灵活地传播与验证。非对称加密用来验证交易的真实性，保障了每个人对财产的所有权。智能合约赋予了区块链灵活的可编程特性，是货币、金融、社会等应用领域得以可编程的重要基础。

2.2、颠覆传统结构，发展尚需实践

区块链节点组合形成去中心化的网络。第一，区块链通过自愿原则建立一套所有节点都可以参与的分布式数据记录体系，实现会计责任的分散化。第二，区块链中每一笔新数据的传播都根据网络 P2P 协议，由每个节点发送给全网其他所有节点，实现分布式传播。第三，区块链让数据存储在所有的参与节点中，并可选择性的实时更新，极大的提升了数据的安全性，数据的可容错性极高。所以，最终构成了大规模的参与者达成共识的数据库记账系统，具有极高的安全性。

图 6：网络类型



资料来源：INNOVALUE，光大证券研究所

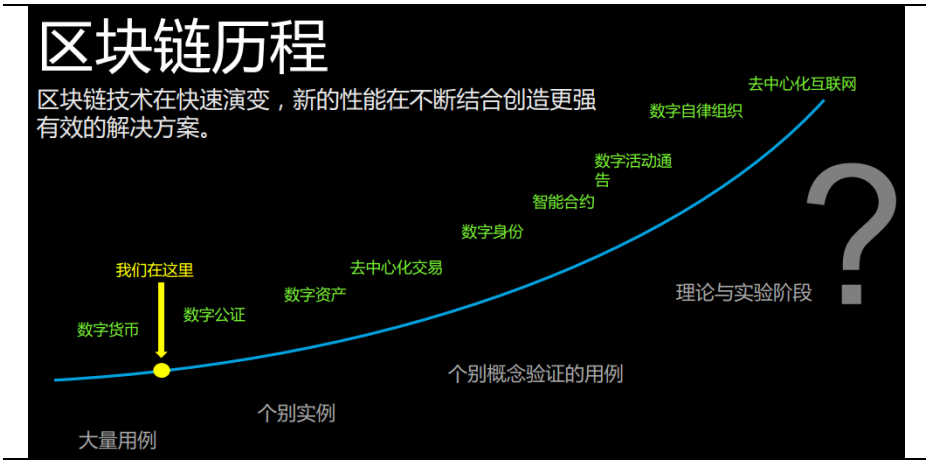
区块链系统从规则和算法上解决了信任问题。一个中心化组织中心机构的主要功能是解决交易双方的信任问题。而在一个区块链系统中，当一个面

向全网所有节点的交易发起时，理论上所有节点都能参与交易响应，但区块链结构的溯源功能使得留存价值不够的节点交易不被承认。同时时间戳代表这个信息是在这个时间写入，保证了信息的真实性和不可篡改性，从而在不需要第三方机构验证节点参与交易能力的基础上实现时间为优的交易达成。而对于一笔点对点的交易发起时，区块链系统通过非对称加密算法保证了全网所有节点能够获取信息，但只有目标节点能够读取信息，从而保证交易的安全性。

区块链具有去中心化、去信任、集体维护和可靠数据库四大特征。区块链系统中一个交易同时有多个节点参与记录，且区块前后相接，一旦一个区块生成并加入链条，若想更改就意味着必须同时更改至少 51%以上的节点该区块的信息才能获得信任，这一点在技术上很难做到，从而保证了信息的不可篡改。同时，区块链的所有交易都是建立在同一套协议的基础之上，交易信息全网公开和可溯源使得交易方的验证在系统内就可以完成而不需要第三方背书，从而实现了去中心化和去信任。此外，为了拓展区块链的延展性，当需要进行另一类交易时，就需要重新定义交易的合约，这一点可以通过可编程的智能脚本来实现。

技术尚处初期，发展尚需实践。区块链分布式结构带来了众多优势，也产生了许多问题。首先，所有节点同时参与记录并将交易信息实时更新并存储，带来了大量的能量消耗和对存储量的要求。其次，一个区块的生成需要系统内多个节点参与记录并验证通过，带来能量浪费的同时也大大延缓了交易达成的时间，比特币系统当前的理论峰值是 7 笔/秒，而支付宝在 2015 年双十一则高达 8.59 万笔/秒，在大规模交易面前区块链系统的承压能力还需要大幅提高。德勤将区块链的应用分成三个阶段：第一阶段是理论探讨阶段；第二阶段是金融机构纷纷建立实验室，开始关注区块链概念技术，并开始用区块链做一些业务测试；第三阶段是大规模应用阶段，区块链真正走到生产系统中去；当前尚处于第二阶段。

图 7：区块链的发展历程展望



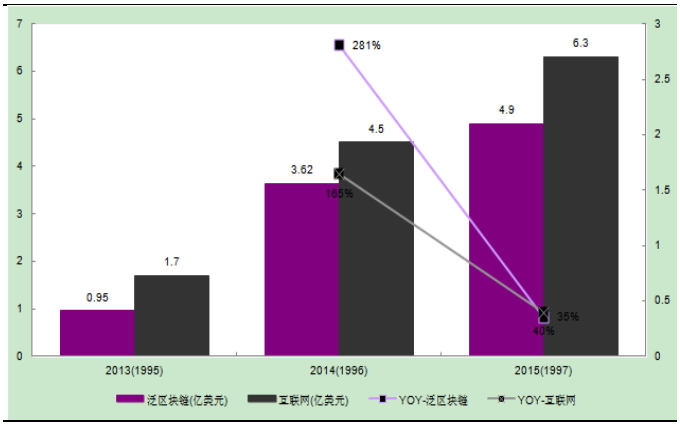
资料来源：德勤

2.3、市值高速增长，市场空间广阔

泛区块链行业的融资金额近年增长明显。据波士顿咨询统计，自 2013 年以来，区块链领域的投资额翻了三倍，目前全球有 750 多家与区块链技术相关的创业公司，其中约 200 家获得了风投注资。2015 年全球共发生数字

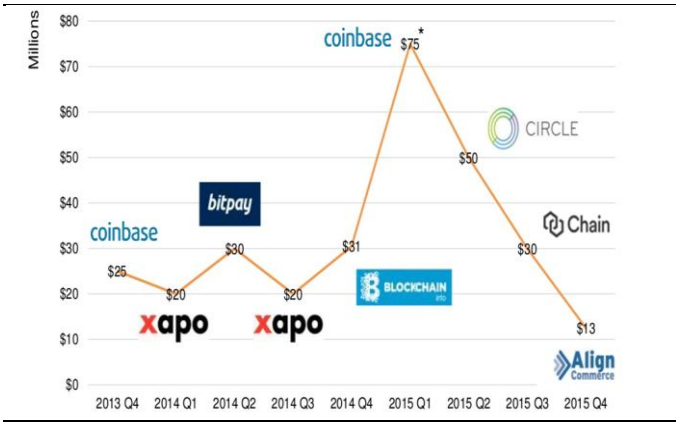
货币/区块链投资事件 65 起，披露金额达到了 4.9 亿美元，较 2014 年总投资额 3.61 亿美元增长 36%，整个行业的累积融资金额已突破 10 亿美元大关。2015 年上半年，Coinbase、21 Inc、Circle 三家公司共计获得 2.41 亿美元巨额融资。虽然融资绝对值并不显眼，但正如互联网初创时期融资情况一样，其意义重大。

图 8：泛区块链与互联网初期融资对比



资料来源：8BTC、CoinDesk，光大证券研究所

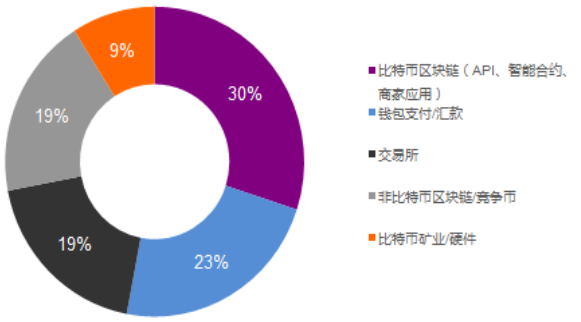
图 9：区块链行业主要融资事件



资料来源：CoinDesk

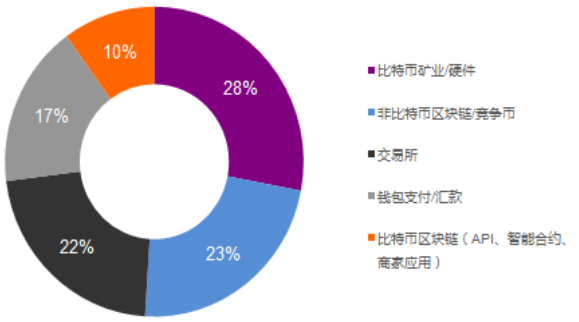
2015 年风险资本总体偏爱比特币，非比特币区块链项目崭露头角。从风险投资流向的细分领域来看，比特币相关项目或公司的融资金额占总融资的 77%，其中又多与交易或挖矿相关。钱包支付/汇款领域投资事件占比 19%，投资额占比 17%；交易领域投资事件占比 19%，投资额占比 22%；矿业硬件领域投资事件占比 9%，投资额占比 28%；比特币区块链(API、智能合约、商业应用等)投资事件占比 30%，投资额占比 10%；非比特币区块链/竞争币领域投资事件占比 19%，投资额占比 23%。

图 10：2015 年数字货币/区块链公司融资次数分布图



资料来源：8BTC

图 11：2015 年数字货币/区块链公司融资金额分布图



资料来源：8BTC

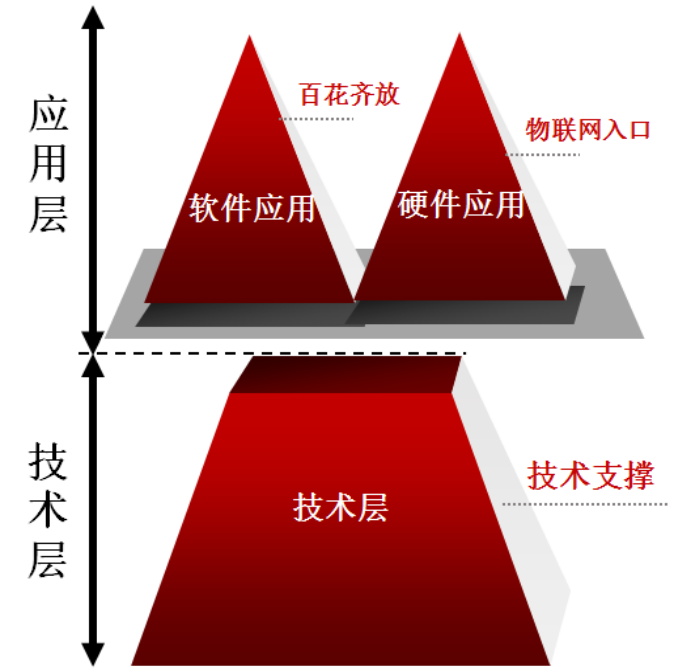
3 年内非比特币资产区块链市值上涨 16 倍。根据数字货币市值排行榜调查报道，截止 2016 年 3 月 20 日，比特币市值目前高居榜首，达到 63.2 亿美元，相应的以太币市值 8.2 亿美元，瑞波市值 2.7 亿美元，莱特币市值 1.4 亿美元。过去三年内，非比特币资产总市值增长了 16 倍，比特币资产市值增长了 3 倍。**根据世界经济论坛调查报告预测，到 2025 年全球 GDP 中有 10%的相关信息将用区块链技术保存。**

3、区块链的系统框架

一般说来，区块链系统框架由数据层、协议层(网络层、共识层、激励层、合约层)和应用层(软/硬件应用)组成。其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等技术；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础;应用层则封装了区块链的各种应用场景和案例*。从应用形态来看，应用层可分为软件应用、硬件应用。从应用范围来看，应用层可分为可编程货币、可编程金融和可编程社会。

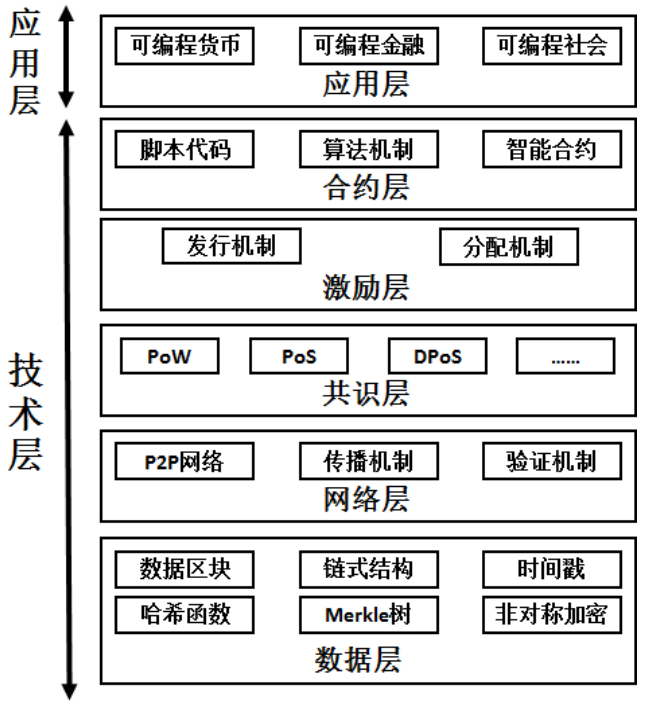
* 引用来源：《自动化学报》。

图 12：区块链层次框架



资料来源：光大证券研究所

图 13：区块链技术层详细体系



资料来源：《自动化学报》

3.1、技术层：区块链账本的技术支撑

■ **典型的技术层项目**

Azure：微软开发的区块链技术平台。微软在 Azure 云平台上已经开始提供“区块链即服务”(BaaS，Blockchain as a Service)，类似一种“沙盘”，合作伙伴可以在一个低风险的环境中与不同技术互动，从智能合约到基于区块链的税务汇报服务。客户既可以直接在 Azure 上使用区块链，也可以通过这个平台在一个本地数据中心中运行区块链。在微软 Azure 的 BaaS 系统中，现有的合作伙伴包括 ConsenSys、Ripple、Eris Industries、CoinPrism、Factom、BitPay、Manifold Technology、LibraTax 和 Emercoin。

Ethereum(以太坊)：一个可灵活编程的区块链技术平台。开发者基于该平台可以快速地部署区块链应用，更加专注于商业逻辑开发，减少开发成本。

它包含一个编程语言，允许用户编写更复杂的智能合约，当货物到达自动支付并打印发票，或如果利润达到一定水平，自动发送给业主股息。在此平台的基础上，企业只需给以太坊区块链设置一些运行的规则即可完成大量交易。在各种各样的方法规则下，车钥匙中嵌入以太坊区块链，就可以被出售或出租，从而产生出租或共享汽车的新模式。

3.1.1、数据层：设计账本的数据结构

■ **数据区块**

区块(block)包含有数据库中实际需要保存的数据，这些数据通过区块包装组织起来被写入数据库。数据通过称为区块的文件，永久记录在数字货币网络上。它们好比是一个股票交易账本。新的区块会被添加到记录(区块链)的末端，而且一旦书写就很难修改或移除。**每个区块由区块头、区块主体组成。区块主体负责记录交易信息，它包含一段时间内所有交易信息，区块头用以实现区块链的其他功能。**

图 14：区块由区块头与区块主体组成

资料来源：互联网

区块头中各数据的含义：

- **父区块哈希值，**32 字节，引用的区块链中父区块头的哈希值，通过这个值每个区块才首尾相连组成了区块链，并且这个值对区块链的安全性起到了至关重要的作用。
- **Merkle 树根，**32 字节，这个值是由区块主体中所有交易信息的哈希值再逐级哈希计算出来的一个数值，主要用于检验一笔交易是否在这个区块中存在。
- **时间戳，**4 字节，记录该区块产生的时间，精确到秒。
- **难度值，**4 字节，该区块相关数学题的难度目标。
- **Nonce，**4 字节，记录解密该区块相关数学题的答案的值。

图 15：区块头的内容

字段名	含义	大小(字节)
Version	版本号	4
HashPrevBlock	上一个block hash值	32
Merkle_root	上一个block产生之后至新block生成此时间内，交易数据打包形成的Hash	32
Timestamp	Unix时间戳	4
Bits	目标值，即难度	4
Nonce	随机数	4

资料来源：8btc.com

图 16：区块主体的内容

子结构名称	作用说明	大小
版本	该比特币协议的版本号	4字节
支出交易数量统计	记录了当前区块中所记录的支出交易数量	大于1字节
比特币支出地址详情	记录了当前区块中比特币支出地址的信息	大于40字节
比特币接收地址详情	记录了当前区块中比特币接收地址的信息	大于40字节
接收交易数量统计	记录了当前区块中所记录的接收的交易数量	大于1字节比特
交易时间戳	以UNIX时间格式记录了当前区块中所记录交易被P2P网络确认的时间	4字节

资料来源：8btc.com

挖矿(创建新区块)的过程就是找到随机数 Nonce,使其满足如下条件:

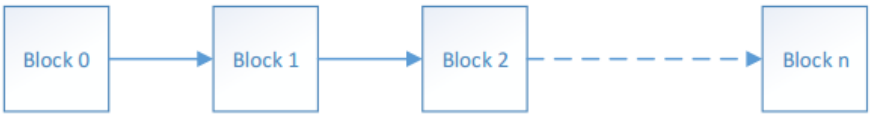
SHA256(SHA256(Version+HashPreBlock + Merkle_root + Timestamp + Bits + Nonce)) ≤ TargetHash

TargetHash(目标哈希值)是由 Bits 经过哈希运算得到的 256 位的数值。SHA256(SHA256(区块头))计算所得哈希值一定要小于或等于目标哈希值，该区块才能被网络所接受，目标哈希值越低，找到随机数 Nonce 产生一个新区块的难度越大。一旦矿工找到了满足条件的随机数 Nonce，就可以广播一个新的区块，其他节点会验证该矿工的区块是否合法。如果矿工的区块被接受，系统会奖励该矿工一定的货币。

■ **链式结构**

每个区块的区块头中记录了其引用的父区块的哈希值，通过这种方式形成了前后区块的链式关系。以比特币为例，区块链中记录的是交易信息，每个节点都在本地保存有一份完整的区块链，每个完整的区块链中都记录了从 2009 年比特币诞生之日起发生的所有交易信息，每当有一个新交易申请产生时，节点都可以通过完整区块链验证这笔新交易的正确性，被验证通过的交易会被记录到下一个将要生成的新区块中。

图 17：链式结构



资料来源：《小蚁白皮书》

● **哈希函数**

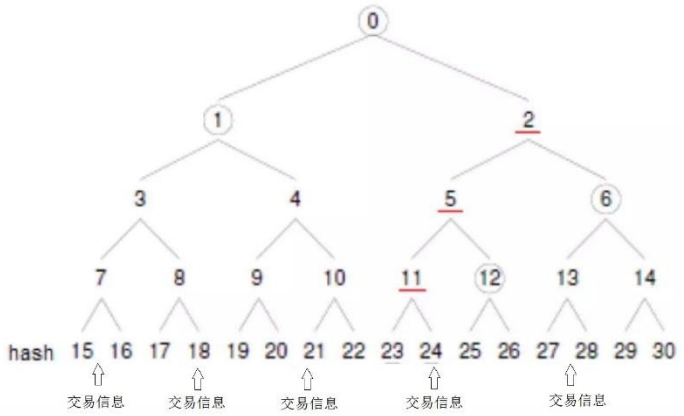
哈希函数将任意长度的二进制值映射为较短的固定长度的二进制值，这个小的二进制值称为哈希值(也可翻译为散列值)。一般来说哈希函数满足这样的关系：f(data)=key，输入任意长度的 data 数据，经过哈希算法处理后输出一个定长的数据 key。这种转换是一种压缩映射，也就是说，哈希值的空间通常远小于输入的空间，是一段数据唯一且极其紧凑的数值表示形式。哪怕一段数据只有很细微的改变，随后的哈希函数都将产生不同的哈希值。要找到哈希值相同的两个不同的输入，在计算上是不可能的。

■ Merkle 树

Merkle 树是一种数据编码的结构。在最底层，我们把交易信息数据分成小的数据块，有相应的哈希值和它对应。但是往上走，并不是直接去运算根哈希值，而是把相邻的两个哈希值合并成一个字符串，然后运算得到这个字符串的哈希值，这样每两个哈希值就结婚生子，得到了一个“子哈希值”。依次往上推，可以得到数目更少的新一级哈希，最终必然形成一棵倒挂的树，到了树根的这个位置，这一代就剩下唯一的根哈希值，我们把它叫做 Merkle 根。

目前在计算机领域，Merkle 树大多用来进行比对以及验证处理。在处理比对或验证的应用场景中特别是在分布式环境下进行比对或验证时，Merkle 树会大大减少数据的传输量以及计算的复杂度。例如，假设 15,16,17.....30 是一个个数据块的哈希值，我们把这些数据从 A 节点传输到 B 节点，并且在数据传输到 B 节点后，我们想验证下传输到 B 节点上的数据的有效性型(验证数据是否在传输过程中发生变化)，我们只需要验证 A 和 B 上所构造的 Merkle 树的根节点值是否一致即可。如果一致，表示数据是有效的，传输过程中没有发生改变。假如在传输过程中，23 对应的数据被人篡改，通过 Merkle 树很容易定位找到(因为此时，树节点 0、2、5、11、23 对应的哈希值都发生了变化)。

图 18：Merkle 树示例



资料来源：互联网，光大证券研究所

■ 非对称加密

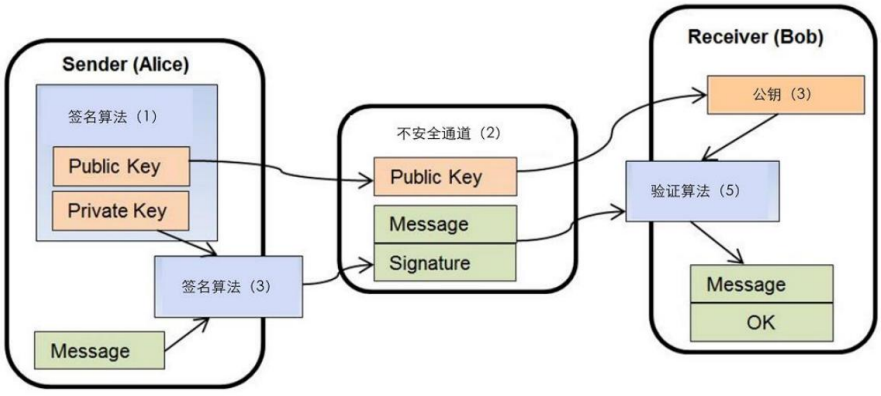
非对称加密算法是一种密钥的保密方法。非对称加密算法需要两个密钥：公钥和私钥。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密，从而获取对应的数据价值；如果用私钥对数据进行签名，那么只有用对应的公钥才能验证签名，验证信息的发出者是私钥持有者。因为加密和解密使用的是两个不同的密钥，所以这种算法叫做非对称加密算法，而对称加密在加密与解密的过程中使用的是同一把密钥。

图 19：对称加密 VS 非对称加密

资料来源：百度百科

基于私钥的数字签名是与纸质文件上的墨水签名有类似功能的数字文件加密技术。他保证签名数字文档由本人生成，没有被篡改。以图中数字签名的使用方案为例，首先 Alice 产生一个密钥对，通过不安全通道（公开通道）将她的公钥给 Bob。然后，她通过签名算法和她的私钥来签署交易信息。最后，她将信息发送给 Bob，Bob 可以使用公钥和一个验证算法来验证该信息。

图 20：数字签名方案

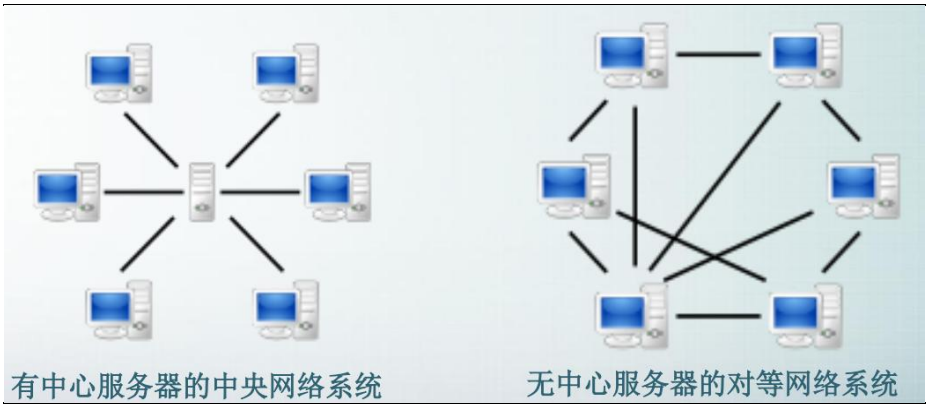


资料来源：UniCredit

3.1.2、网络层：实现记账节点的去中心化

对等网络（peer-to-peer，P2P），又称点对点技术，是没有中心服务器、依靠用户群交换信息的互联网体系。与有中心服务器的中央网络系统不同，对等网络的每个用户端既是一个节点，也有服务器的功能。其具有去中心化与健壮性等特点。一、去中心化：网络中的资源和服务分散在所有结点上，信息的传输和服务的实现都直接在结点之间进行，可以无需中间环节和服务器的介入。二、健壮性：P2P 架构天生具有耐攻击、高容错的优点。由于服务是分散在各个结点之间进行的，部分结点或网络遭到破坏对其它部分的影响很小。

图 21：中央网络系统 VS 对等网络系统



资料来源：互联网

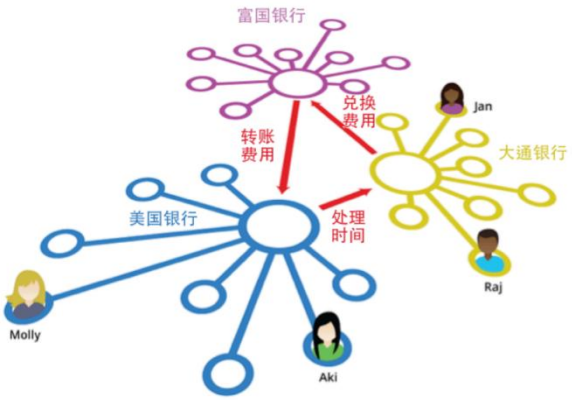
比特币网络被设计为能高效且灵活地传播数据至所有节点的模式。一笔传递到比特币网络中任意节点的交易数据会被发送到三至四个相邻节点，而每一个相邻节点又会将交易数据发送到三至四个与其相邻的节点。以此类推，在几秒钟之内，一笔有效的交易就会以指数级的速度在网络中传播，直到所有连接到网络的节点都接收到它。

比特币网络每一个节点在传播数据之前均进行独立的数据验证。每一个节点在校验每一笔交易时，都需要对照一个长长的标准列表(语法结构是否正确，字节大小是否符合要求，账户余额是否冲突……)。如果交易被验证有效，该节点会将这笔交易传播到所连接的其他节点；同时，交易发起者会收到一条表示交易成功的返回信息。如果这笔交易被验证为无效，这个节点会拒绝接受这笔交易且同时返回给交易发起者一条表示交易被拒绝的信息。

- **Ripple**

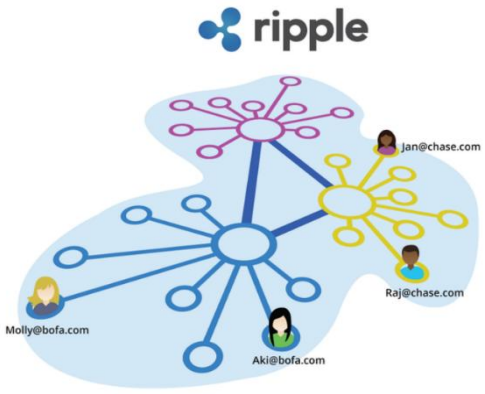
Ripple 是一种用以进行点对点金融交易的互联网协议。互联网协议是网络上的节点为了协助互相通讯所遵守的一套规则。Ripple 协议可以让不同的支付体系进行交流，实现节点间的数据传输与验证流程的标准化，进行直接、即时的交易，降低结算费用。正如同 SMTP 为电子邮件创造了一个共享的标准环境一样，Ripple 也为支付创造了共享的标准。Ripple 和电子邮件一样，是无主的，没有中心管理者，可以帮助全世界的服务器节点互相进行点对点金融交易。以类似协议作为金融交易的标准协议，支付就会变得如同节点间收发电子邮件一样更加快捷、便宜而简单，收付都即时进行。

图 22：现在的金融支付系统



资料来源：Ripple

图 23：Ripple 是一个点对点的支付协议



资料来源：Ripple

3.1.3、共识层：调配记账节点的任务负载

■ **工作量证明机制(Proof of Work, POW)**

工作量证明机制挑选能够计算出一个满足规则的随机数的节点，赋予其新区块产生时的记账权。通俗地说，节点获得多少货币，取决于其挖矿贡献的有效工作。也就是说，节点的电脑性能越好，计算出随机数的可能性越大，获得创建新区块权利的可能性越大，分给该节点的矿就会越多，这就是根据节点的工作证明来执行货币的分配。大部分的虚拟货币，比如比特币、莱特币，都是基于 POW 模式的虚拟货币。

■ **股权证明机制(Proof of Stake, POS)**

股权证明机制已有很多不同变种，但基本概念是获得对新区块记账权利的可能性与该节点在网络里所占的股权(所有权占比)成比例，等比例地降低挖矿难度。点点币(Peercoin)和未来币(NXT)均使用这一机制。点点币使用一种混合模式，用节点的股权来调整其挖矿难度。未来币使用一个确定性算法以随机选择一个节点来对下一个区块记账，该算法基于节点的账户余额来调整其被选中的可能性。

■ **授权股权证明机制(Delegate Proof of Stake，DPOS)**

授权股权证明机制的理念是每个节点可以将其投票权授予一名代表，获票数最多的前 100 位代表按既定时间表轮流记录产生的区块。每名代表分配到一个时间段来生产区块，所有的代表将收到等同于一个平均水平的区块所含交易费的 1%作为报酬。如果一个平均水平的区块含有 100 股作为交易费，一名代表将获得 1 股作为报酬。从某种角度来看，DPOS 像是美国的议会制度，如果代表不能履行他们的职责(当轮到他们时，没能记录新生成的区块)，他们会被除名，网络会选出新的超级节点来取代他们。

表 1：不同共识机制的优缺点对比

共识机制	优点	缺点
POW	完全去中心化，节点自由进出。	挖矿造成大量的资源浪费，共识达成的周期较长，不适合商业应用。
POS	在一定程度上缩短了共识达成的时间。	还是需要挖矿，本质上没有解决商业应用的痛点。
DPOS	大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。	削弱了去中心化属性

资料来源：互联网

3.1.4、激励层：制定记账节点的“薪酬体系”

■ **发行机制，激励机制：以比特币为例**

比特币最开始由系统奖励给那些创建新区块的矿工，该奖励大约每四年减半。比特币系统每 10 分钟产生一个新区块，即每 10 钟有新的比特币奖励给矿工，这是货币发行的方式。这受控制的供应发行，意味着所有的比特币(系统设置的比特币总量：2100 万)最终会被开采出来，并且所有的币将永远都可用。刚开始每记录一个新区块，奖励矿工 50 个比特币，该奖励大约每四年减半。依次类推，到公元 2140 年左右，新创建区块就没有系统所给予的奖励了。**届时比特币全量约为 2100 万个，这就是比特币的总量，所以不会无限增加下去。**

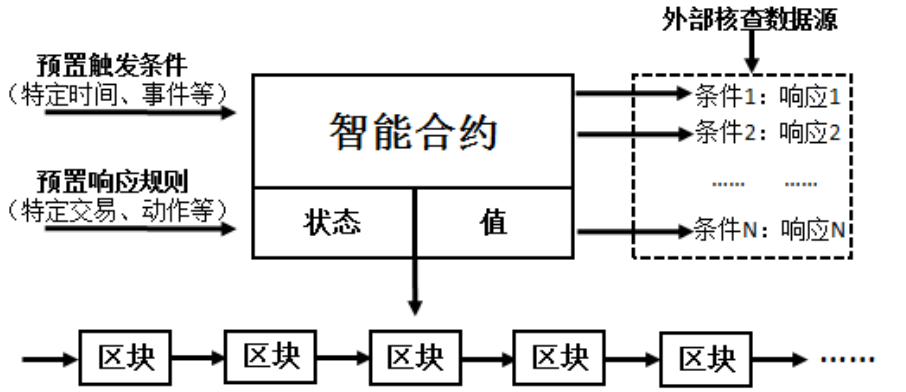
另外一个激励的来源则是交易费。新创建区块没有系统的奖励时，矿工的收益会由系统奖励变为收取交易手续费。例如，你在转账时可以指定其中

1%作为手续费支付给记录区块的矿工。如果某笔交易的输出值小于输入值，那么差额就是交易费，该交易费将被增加到该区块的激励中。只要既定数量的电子货币已经进入流通，那么激励机制就可以逐渐转换为完全依靠交易费，那么就不必再发行新的货币。

3.1.5、合约层：赋予账本可编程的特性

智能合约是一组情景应对型的程序化规则和逻辑，是通过部署在区块链上的去中心化、可信共享的脚本代码实现的。通常情况下，智能合约经各方签署后，以程序代码的形式附着在区块链数据(例如一笔比特币交易)上，经 P2P 网络传播和节点验证后记入区块链的特定区块中。智能合约封装了预定义的若干状态及转换规则、触发合约执行的情景(如到达特定时间或发生特定事件等)、特定情景下的应对行动等。区块链可实时监控智能合约的状态，并通过核查外部数据源、确认满足特定触发条件后激活并执行合约。

图 24：智能合约结构

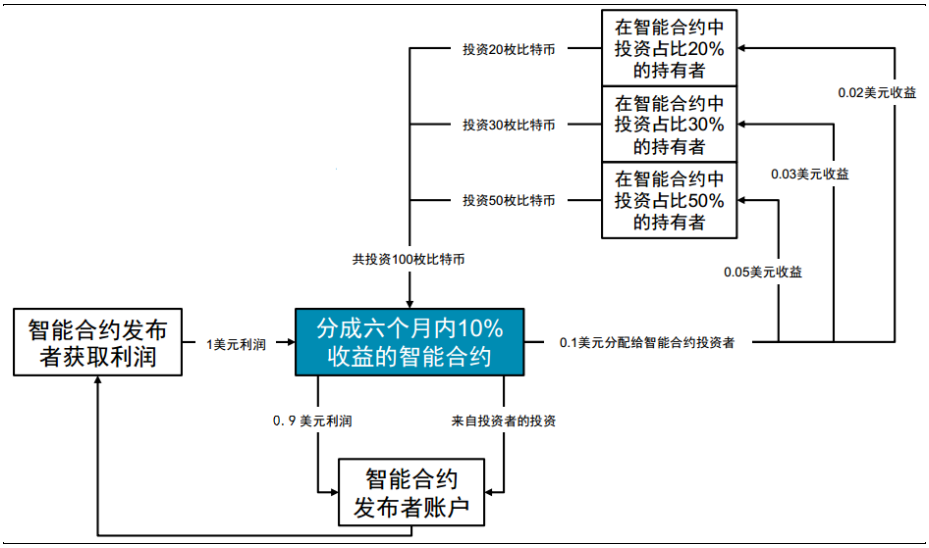


资料来源：《自动化学报》

智能合约的优势是利用程序算法替代人执行合同。这些合约需要资产、过程、系统的自动化组合与相互协调。合约包含三个基本的要素：要约、承诺、价值交换，如果存在一个出价行为、接受行为以及价值交换的行为，那么就是一个合约，因此可以适用合同相关的法律。一些合约必须以书面的形式写下来，但很多是不需要的，可交由程序去自动执行。

智能合约的内容可能是一组写入网络的合同条款，这些条款由程序基于合法数据进行校验，并自动执行。仍以比特币为例：首先，用户 A 为了筹集比特币，创建并发布一份智能合约，内容是会把他在比特币的投资中获得的 10%利润分红给他的投资者，共有 3 位投资者够买了这一合约，分别是 20、30 和 50 比特币(或等值货币)。当用户 A 在交易中获取了 1 美元的利润后，其中的 10%，也就是 0.1 美元，将会按照投资比例分红给三位投资者。这是一个常规的分红过程，但是智能合约支持下，分红的过程可由计算机自动执行、进行点对点的转账等操作。

图 25：智能合约示例



资料来源：Accenture

智能合约技术的主要发展趋势是由自动化向智能化方向演化。现存的各类智能合约及其应用的本质逻辑大多仍是根据预定义场景的“如果-那么”类型的条件响应规则，能够满足目前自动化交易和数据处理的需求。未来的智能合约应具备根据未知场景的推演、计算和一定程度上的自主决策功能，从而实现由目前“自动化”合约向真正的“智能”合约的飞跃。IBM 提出了一种 Watson 驱动的区块链设想，这种区块链特色之一就是让设备所有者在区块链上注册，让机器来创建智能合约、决定不同层次的访问、为不同用户提供个性化功能。

智能合约对于区块链技术来说具有重要的意义。一方面，智能合约使区块链的灵活性大幅提升，为静态的底层区块链数据赋予了灵活可编程的机制和算法，并为构建区块链时代的可编程金融系统与社会系统奠定了基础。另一方面，智能合约的自动化和可编程特性使其可封装分布式区块链系统中各节点的复杂行为，成为区块链构成的虚拟世界中的软件代理机器人，这有助于促进区块链技术在各类分布式人工智能系统中的应用，使得基于区块链技术构建各类去中心化应用、去中心化自治组织、去中心化自治公司甚至去中心化自治社会成为可能。

■ **公司应用案例**

以太坊：近日快速崛起，一个重要的推动因素是它将区块链和智能合约技术实现了良好的结合。智能合约就是在资产内植入一些代码，这些代码可以自动智能决定网络中相关资产运作的地点和方式。以太坊致力于打造一个提供复杂脚本语言的优秀底层协议。在该协议的基础上，区块链结合智能合约可以打开大面积商用空间，用户可以创建任意的高级智能合约，例如：众筹协议、货币、投票、金融衍生品、公司管理应用等。

德国初创公司 Slock.it 想做一个基于区块链技术的智能锁，将锁连接到互联网，通过区块链上的智能合约对其进行控制。任何一个控制锁的人可以发放一把或多把私钥，并对私钥进行复杂的定制，设定锁什么时候启用、具体什么时候打开等。通过这种方式，共享经济能够被进一步去中心化，将任何能被锁起来的东西轻易租赁、分享和出售。Slock 让使用者能够直接向一

把锁进行支付，然后打开；出租者也可以在房客走后随时更换私钥的定制，让整个体验更为方便、安全；人们也可以通过使用这一技术进行自行车、密码柜的租赁等，甚至让他人在自家门口给车充电，然后收取费用等。

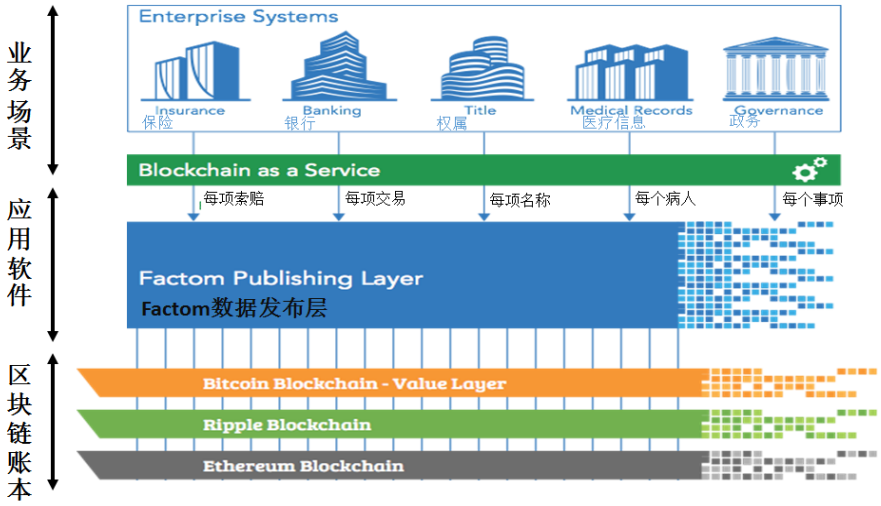
3.2、应用层：连接业务场景与区块链账本的桥梁

3.2.1、软件应用：百花齐放

■ **以 Factom 为例**

Factom 作为业务场景与多个区块链账本之间的中间层，提供一种灵活的访问方式。上层的业务基于 Factom 区块链引擎提供的 API，把验证审查过的数据发布到区块链账本上。通过这种封装和类似于中间件的做法，显著降低上层业务连接到区块链账本的难度。

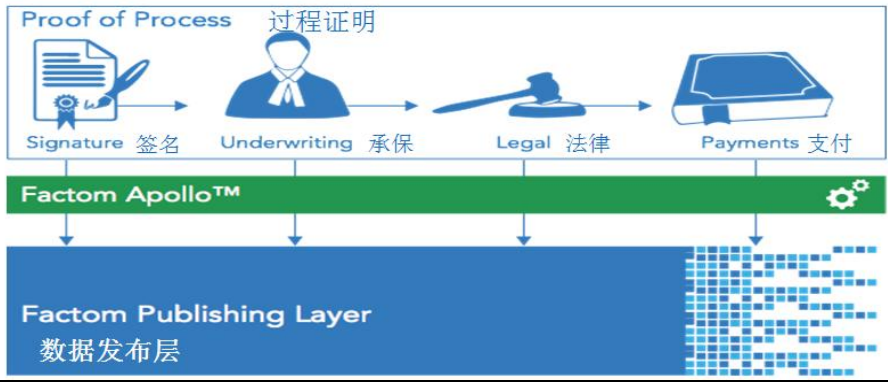
图 26：Factom 整体的工作体系



资料来源：Factom，光大证券研究所

Factom 对业务环节确认后，将业务数据转到发布层保存。Factom 可以用在供应链管理、物流、金融、医疗等领域，依靠计算机网络的可靠执行，克服人类大脑遗忘、自我欺骗等等缺点，让共识规则和业务流程可以有序执行、完备执行。通过把签名、担保、法律保护、以及信用证支付结合在一起的处理方式，使一环扣一环的业务数据进入到 Factom 的数据发布层并加以保存。

图 27：Factom 对业务环节的执行确认



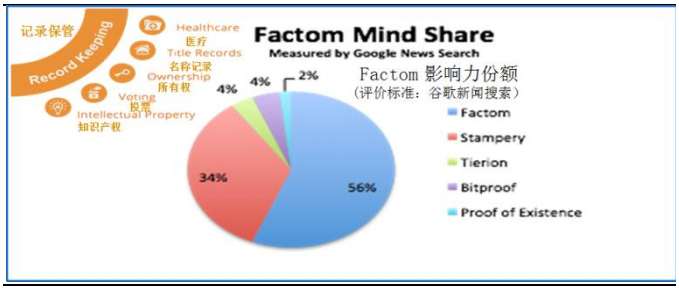
资料来源：Factom

Factom 最后把发布层的数据注入区块链账本。如果 Factom 出了问题怎么办？出于更多冗余的考虑和防止 Factom 作恶的目的，数据永久性可以通过将数据注入到更多的区块链账本上来解决。作为一个数据链路层，Factom 可以与任意底层的区块链账本建立联系，协助把数据指纹注入到底层区块链账本上，通过多重冗余，确保数据的永久性。

图 28：保证数据永久性

资料来源：Factom

图 29：Factom 在记录保管领域市场影响力最大



资料来源：Factom

3.2.2、硬件应用：物联网的入口

■ **Filament：传感器设备**

Filament 公司提出了他们的传感器设备，它允许以秒为单位快速地部署一个安全的、全范围的无线网络，设备能直接与其它的 10 英里内的设备通信，而且可以直接通过手机、平板或者电脑来连接。通过以区块链为基础的技术堆栈操作，Filament 设备能够独立处理付款，并能允许智能合约确保交易的可信。

图 30：Filament 传感器设备概念示意图

资料来源：LetsTalkPayments.com

■ **Ken Code：ePlug**

ePlug 是 Ken Code 公司的一款产品，它是一个小型电路板。为了安全性与可靠性，该产品提供了可选的分布式计算、端到端的数据加密方式、无线连接、定时器、USB 接口、温度传感器、触觉传感器、光线和运动传感器等功能，该产品以基于区块链的登陆方式来确保安全，一旦输入正确的网络地址，ePlug 所有者会进入一个登陆界面进行身份验证。

图 31：ePlug 示意图

资料来源：Ken Code

4、区块链应用发展的三个阶段

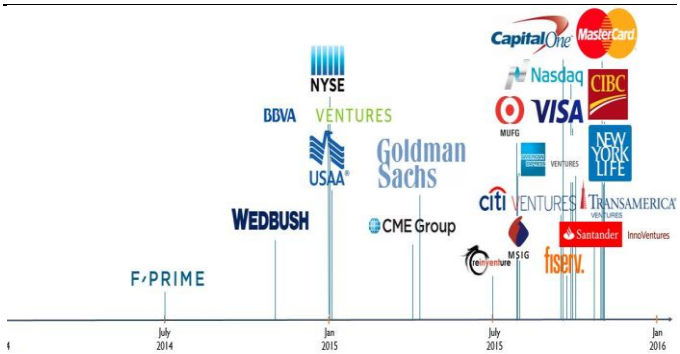
Melanie Swan 在书籍《区块链—新经济蓝图》一书中将区块链的应用层次划分为 1.0、2.0 和 3.0 三个阶段：区块链 1.0 是可编程货币，是与转账、汇款和数字化支付相关的密码学货币应用；区块链 2.0 是可编程金融，是经济、市场和金融领域的区块链应用，例如股票、债券、期货、贷款、抵押、产权、智能财产和智能合约；区块链 3.0 是可编程社会，是超越货币、金融和市场的应用，特别是在政府、健康、科学、文化和艺术领域的应用。我们也借助这三个层次对区块链的应用领域进行展开。

4.1、区块链 1.0：可编程货币

4.1.1、搅动金融市场

区块链技术在金融领域备受瞩目。大型金融机构诸如纽交所、高盛、芝交所、花旗、纳斯达克等等都在过去的一年中进入了区块链领域。目前全球 42 家大型银行已经加入了区块链联盟 R3，其核心任务是进行区块链技术的概念验证和相关技术标准的制定。同时，区块链在证券市场的潜力也引起了各大证券交易所的重视。在纳斯达克公布区块链平台 Linq 以后，欧洲证券市场的机构纷纷跟进。2015 年 11 月 17 日，伦敦证券交易所、伦敦清算所、法国兴业银行、瑞银集团(UBS)以及欧洲清算中心(Euroclear)等机构联合成立了区块链集团，探索区块链技术如何改变证券交易的清算和结算方式。据世界经济论坛预测，到 2027 年世界 GDP 的 10%将被存储在区块链网络上。

图 32：2014 年以来，金融机构纷纷介入区块链领域



资料来源：CB INSIGHTS

图 33：R3 联盟已吸引了全球 42 家银行加入

资料来源：CoinDesk

■ **银行业：成立区块链联盟 R3**

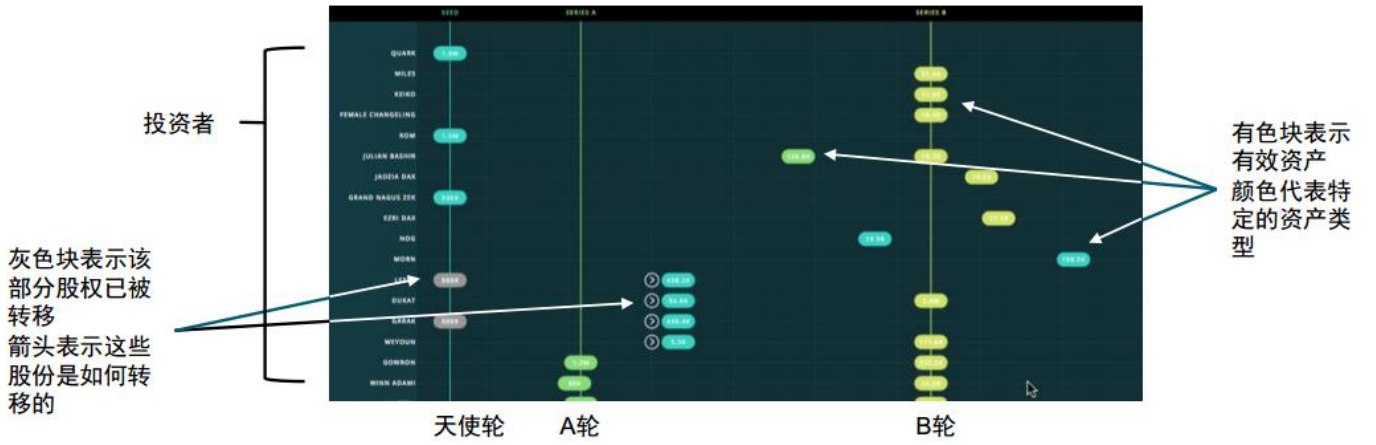
R3 联盟是由分布式账本初创公司 R3CEV 建立了一个有 42 家金融机构参与的金融联盟，包括巴克莱银行、瑞士信贷银行、高盛投资集团、美国合众银行、丹麦银行、富国银行、荷兰国际集团、日本瑞穗实业银行、瑞典北欧联合银行、意大利联合信贷银行等金融巨头。R3CEV 认为通过三项服务可以解决金融联盟成员的需求。第一项服务是创建技术基础层结构，并计划在上面构建各种的应用案例和私有区块链。第二项服务是全球协作实验室，参与者要通过严苛的业务流程，包括申请、测试和分析三个阶段。第三项服务是根据全球协作实验室发现的成功应用案例，在基础技术结构层上建立商业应用模式*。

* 引用自《全面认识区块链私有区块链》。

■ **证券业：推出的基于区块链的证券交易系统 Linq**

Linq 是纳斯达克推出的基于区块链的证券交易系统，它主要用于私人公司的股权交易。2016 年 1 月，美国证券交易委员会批准在线零售商 Overstock.com 提交的 S-3 申请，允许将该公司的新上市股票在比特币区块链上交易并实现了首个成功应用。纳斯达克私人股权市场是在 2014 年推出的，这是交易所最新的一次尝试来进入在 Pre-IPO 阶段让二级市场进行股权交易，随着越来越多的初创公司选择保留更长时间处于私人公司阶段，这意味着 IPO 之前的交易变得再次令人关注，因为投资者希望能够获得一些流动性，也可以减少早期阶段管理层的压力。无疑 Linq 是纳斯达克拓展在私募股权交易领域的有益尝试。

图 34：Linq 股权时间轴图



资料来源：Accenture

4.1.2、构建新型货币体系

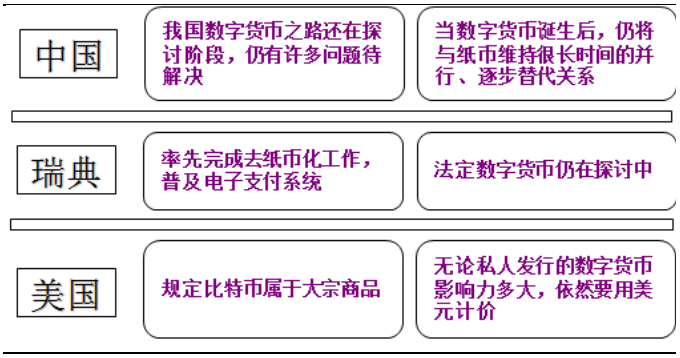
数字货币不同于电子货币。当前数字货币(digital money)尚没有统一定义，反洗钱金融行动特别工作组(FATF)认为数字货币是一种价值的数据表现形式，通过数据交易并发挥交易媒介、记账单位及价值存储的功能，但它并不是任何国家和地区的法定货币，也没有政府当局为它提供担保，只能通过使用者间的协议来发挥上述功能。而电子货币是将法定货币数字化后以支撑法定货币的电子化交易，因此二者并不等同。目前数字货币的主流是以比特币为代表的去中心化的数字货币。

基于区块链的数字货币体系可以解决传统货币体系的三大弊端。第一，区块链体系是由大家共同维护的，不需专门消耗人力物力，去中心化结构使得成本大幅降低，同时数据的公开使得在其中做假账不再可能。第二，区块链以数学算法作为背书，所有的规则都建立一个公开透明的数学算法之上，能够让所有不同政治文化背景的人群获得共识，实现了跨区域互信问题。第三，区块链系统中任一节点的损坏或者失去都会不影响整个系统的运作，具有极好的健壮性。

图 35：数字货币相较纸币的优势

资料来源：凤凰财经，光大证券研究所

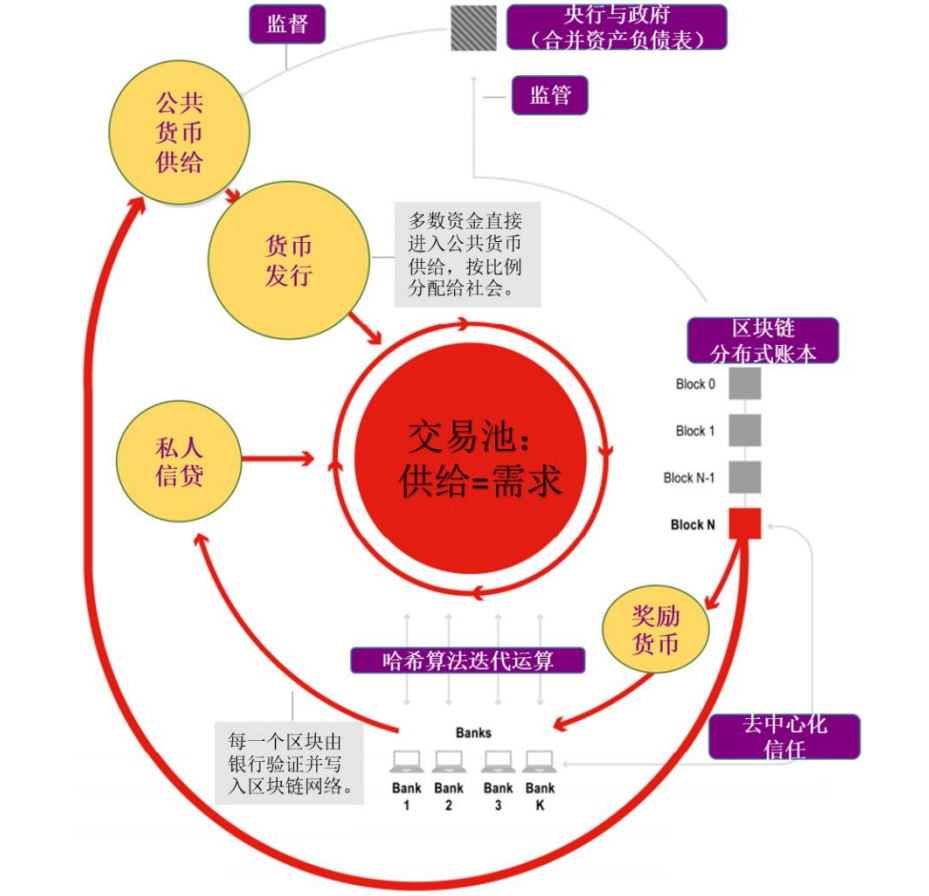
图 36：数字货币进展现状



资料来源：凤凰财经，光大证券研究所

区块链被多家央行视为实现数字化货币的关键技术。英国央行今年宣布将发布数字货币 RSCoin 代码并进行测试，这是一款完全基于央行的需求而设计的基于区块链技术的数字货币，目前由伦敦大学学院(UCL)研发并进入了初步测试阶段。同时荷兰央行正在致力于开发一种被称为“DNBCoin”的内部区块链原型，韩国、俄罗斯央行也表示密切关注区块链技术。此外，2016 年 1 月 20 日，央行发布消息称，数字货币研讨会在北京召开，将探索发行数字货币并表态：发行数字货币可以降低传统纸币发行、流通的高昂成本，提升经济交易活动的便利性和透明度，减少洗钱、逃漏税等违法犯罪行为，加强央行对货币供给和货币流通的控制力。

图 37：基于区块链的数字货币发行流程



资料来源：HSBC，光大证券研究所

数字货币与法币将逐渐融合。从历史发展的趋势来看，货币从来都是伴随着技术进步、经济活动发展而演化的，从早期的实物货币、商品货币到后来的信用货币，都是适应人类商业社会发展的自然选择。法币作为由一个中心化主体发行的货币，较好的解决了货币的信用难题，但同时也带来了成本高、效率低、安全性依赖于中心化主体等问题。而随着互联网的发展，贸易全球化带来支付全球化的变化，数字货币发行、流通体系的建立，对于金融基础设施建设、推动经济提质增效升级，都是十分必要的。

4.2、区块链 2.0：可编程金融

除了构建货币体系之外，区块链在泛金融领域还有众多应用机会。基于区块链可编程的特点，人们尝试将智能合约添加到区块链系统中，形成可编程金融。智能合约的核心是利用程序算法替代人执行合同。这些合约需要自动化的资产、过程、系统的组合与相互协调。合约包含三个基本的要素：要约、承诺、价值交换，并有效定义了新的应用形式，使得区块链从最初的货币体系拓展到金融的其他应用领域，包括在股权众筹、证券交易等领域开始逐渐有应用落地。传统金融机构也在大力研究区块链技术，以期与传统金融应用相结合。

■ **股权众筹**

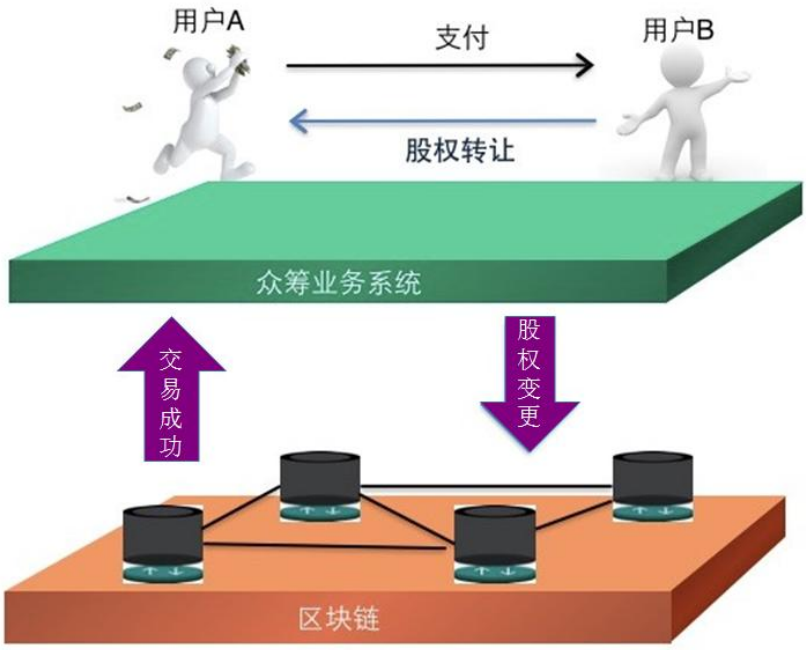
区块链技术在股权众筹领域具备优势。第一，是更加公开透明和真实可信，信息对投融资各方更加对称，记录难以篡改、伪造、删除；第二，促进

股权流通和资源共享，股权转让和登记更安全便捷，众筹平台之间投资人和项目可共享。

股权登记管理：区块链独特的身份账户体系，可以作为电子凭证。现有非上市股权管理，通常情况下，需要通过人工处理纸质股权凭证、期权发放和可换票据。如果出现频繁的股权变更，股东名册的维护将变得繁琐，历史交易的维护和跟踪也变得困难。区块链技术将会对这一切进行数字化管理，使其变得更加高效和安全。区块链众筹股权登记，将充分利用区块链账本的安全透明、不可篡改、易于跟踪等特点，记录公司股权及其变更历史。

股权转让流通：区块链技术可以降低信用风险。传统的 OTC 场外股权交易，以交易双方的信用为基础，由交易双方自行承担信用风险，需要建立双边授信后才可进行交易，而交易平台集中承担了市场交易者的信用风险。应用区块链技术后，股权的所有权登记在区块链中，股权交易必须要所有者的私钥签名才能验证通过；交易确认后，股权的变更也会记录在区块链中，从而保障交易双方的利益。

图 38：基于区块链的股权转让

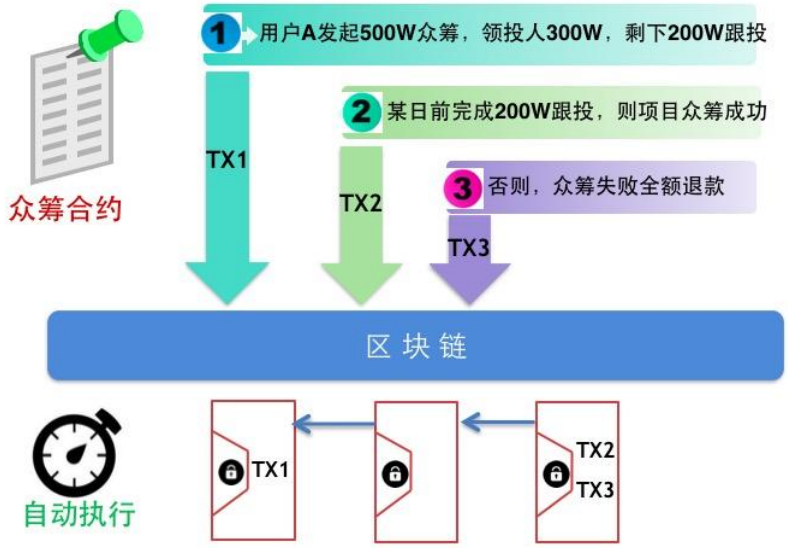


资料来源：《区块链，新经济蓝图及导读》

众筹合约：区块链确保合约履行中不得被篡改。在股权众筹发起初期，由发起人、众筹平台、领投人、保荐人等多方共同签署一份众筹合约，来约定各自的责任与义务。这份合约可以变成智能合约的形式存入区块链中，由区块链确保合约履行中不得被篡改。

区块链众筹合约示例。根据合约的条件，区块链底层首先产生第一个事务(TX1)：创建一个联名账户，从领投人账户打款 300 万到联名账户，并生成 200 万的借条供投资人购买，该账户由合约中各方共同拥有和维护；同时创建 TX2(在规定时间内，如 200 万借条销售完，则从联名账户打款 500 万到发起人账户中)和 TX3(如众筹失败，跟踪联名账户的交易记录，全额退款)。TX1、TX2、TX3 在同一时间写入区块链，由区块链底层自动执行。

图 39：区块链众筹合约示例

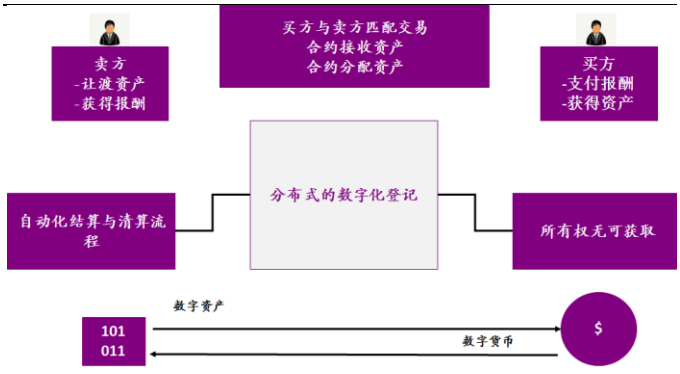


资料来源：互联网

■ **证券交易与发行**

基于区块链的证券交易将大幅节省交易费用。以证券的交易结算为例，使用区块链系统，买方和卖方能够直接实现自动配对，并通过分布式的数字化登记系统，自动实现结算和清算。由于录入区块的数据不可撤销且能在短时间内被拷贝到每个节点中，录入到区块链上的信息实际上产生了公示的效果，因此交易的发生和所有权的确认不会有任何争议。而在证券发行过程中，传统模式下公司想要 IPO，需要有专门的审核流程并由投行机构进行承销。而如果采用区块链技术来实现这个过程，就不需要任何中央机构来运营和管理，交易过程完全公开透明，能够真正实现点对点的交易。

图 40：区块链应用于证券结算和清算领域



资料来源：《当代金融家》

图 41：区块链应用于证券发行领域

资料来源：互联网

4.3、区块链 3.0：可编程社会

区块链是价值互联网的内核。区块链能够对于每一个互联网中代表价值的信息和字节进行产权确认、计量和存储，从而实现资产在区块链上可被追踪、控制和交易。价值互联网的核心是由区块链构造一个全球性的分布式记账系统，它不仅仅能够记录金融业的交易，而是几乎可以记录任何有价值的能以代码形式进行表达的事物：对共享汽车的使用权、信号灯的状态、出生和死亡证明、结婚证、教育程度、财务账目、医疗过程、保险理赔、投票、

能源。因此随着区块链技术的发展，其应用能够扩展到任何有需求的领域，包括审计公证、医疗、投票、物流等领域，进而到整个社会。

■ **审计公证**

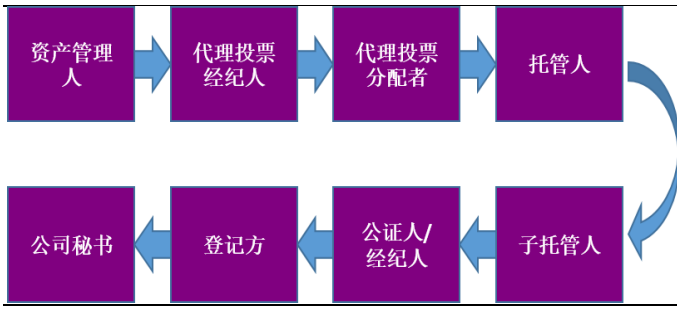
区块链提供了一个分布式的机制进行数据锁定，使数据可以被核查和独立审计。在过去，记录靠手工完成，数据的保护，同步更新和真实性的验证都非常困难。电子化后，由于电脑记录容易被更改，数据核查难题依旧没有解决。而 Factom 协议有效地解决了这一问题，它是基于区块链协议而构建的一层分布式的、匿名的数据协议，维护了一个永久不可更改的、基于时间戳记录的区块链数据网络，大大减小了独立审计、管理真实记录、遵守政府监管条例的成本和难度。商业社会和政府部门可以利用其简化数据管理与记录的流程，并解决数据记录的安全和符合监管的问题。

■ **代理投票**

目前广泛运用的股东代理投票机制程序繁杂。通常资产管理人向代理投票经纪人发出投票指令，指令随后被传递给投票分配者，再由投票分配者将指令传递给托管人以及子托管人。托管人请求公证人对投票指令进行公证，然后向登记方申请并完成登记，最后投票信息汇总到公司秘书处。这是一个非常复杂且非标准化的流程，投票信息存在被不正确传递或丢失的风险。此外，由于托管人及子托管人使用不同的传输系统和字符识别系统，导致投票的追溯和确认非常困难。荷兰一家研究机构就代理投票进行的研究成果指出，在荷兰使用代理投票系统的公司中，仅仅 31%的公司能够确认自己代理投票的结果。

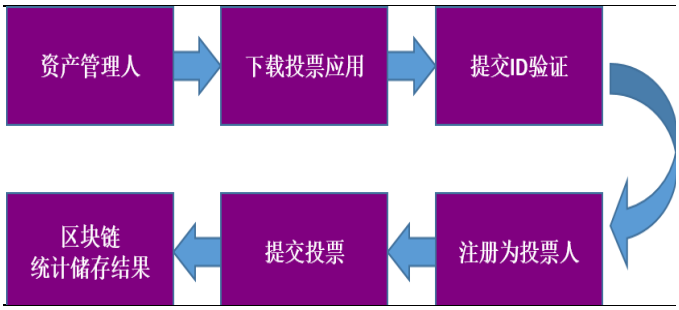
区块链技术可以优化股东代理投票流程。资产管理人只需下载投票软件，提交身份信息并完成注册，即可直接提交投票。投票结果一旦被成功提交至分布式数字化的投票登记系统后将不能再被撤销，同时由于区块链上数据的同步性，资产管理人可以很快地查询到投票结果。这一投票流程较传统模式节省 50%~60%的成本，且同时具有安全、透明、高效、便捷的属性。纳斯达克 OMX 首席执行官 Robert Greifeld 表示，纳斯达克将很快上线区块链代理投票应用，人们将能够在手机上投票并永久享有投票记录。

图 42：传统代理投票



资料来源：德勤，光大证券研究所

图 43：基于区块链技术的代理投票



资料来源：德勤，光大证券研究所

■ **医疗**

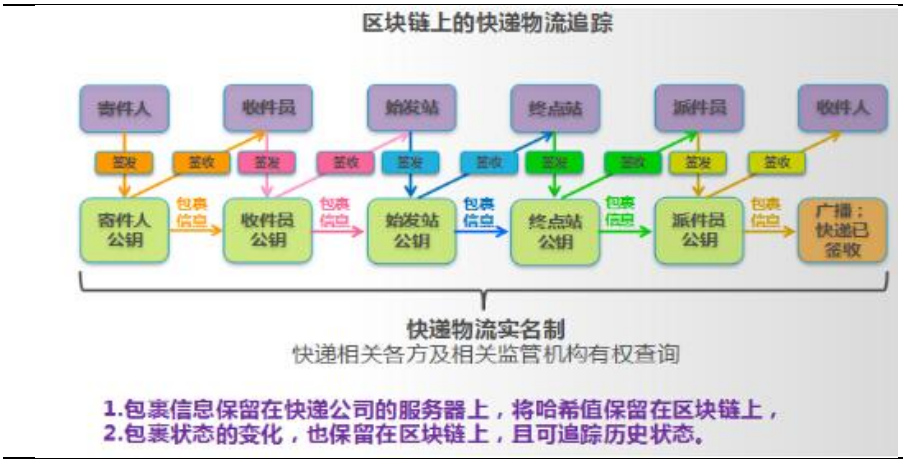
医疗记录尤其是敏感的医疗信息保密对于病人而言是刚性需求，但现实当中这些本该高度保密的信息往往会流入到广告商、黄牛等手中。区块链技术的保密性为医疗信息安全问题提供了解决方法。未来，病人将会拥有属于自己的独立区块链，通过多重签名，防止医院单方面泄露自己的私人信息。

飞利浦医疗保健集团正在与 Tierion 公司进行区块链技术合作，试图寻找到颠覆传统的契机。

■ **物流**

区块链技术可以记录货物从发出到接受过程中的所有环节。通过创建共识网络，能直接定位到快递中间环节的问题所在，也能确保信息的可追踪性，从而避免的快递爆仓丢包、误领错领等问题的发生，也可有效的促进物流实名制的落实。快递交接需要双方私钥签名，每个快递员或快递点都有自己的私钥，是否签收或交付只需要查下区块链即可，最终用户没有收到快递就没有签收，快递员无法伪造签名，杜绝快递员通过伪造签名来逃避考核，减少用户的投诉。

图 44：区块链上的快递物流追踪



资料来源：互联网

5、投资建议

区块链领域的商业模式主要包括生态平台、垂直应用和第三方技术提供方等。伴随软件开源的趋势和技术的普及，区块链底层的技术将不再是门槛，预计将衍生出大量提供第三方区块链技术服务的企业，通过项目制的方式获取收入。与此同时，发展较早并且汇聚了大量应用开发者的技术平台提供方诸如以太仿将逐渐形成平台生态，通过定制开发等增值服务以及交易分成等方式获取收入。此外，在应用领域，无论是基于私链还是公链的应用将会百花齐放，或将颠覆传统的利益格局，在帮助交易各方提高效率降低成本的过程中获取创造价值的部分收入。

区块链发展目前处于第二阶段：金融机构纷纷建立实验室，开始关注区块概念技术，并开始用区块链做一些业务测试。比如 R3 区块链联盟的成立，央行在进行区块链技术的研究，万向区块链实验室的设立，一些基于区块链技术的商品可溯源项目的落地，以及一些 A 股上市公司公开宣称在研究区块链相关技术。结合国内区块链领域的发展现状，我们认为将区块链技术应用到垂直领域未来或将大放异彩，尤其是目前对区块链技术参与度最高的金融领域，**潜在的实践者包括金融 IT 公司和第三方支付企业，重点推荐海立美达、广电运通和御银股份。建议关注恒生电子、赢时胜、飞天诚信。**

6、风险提示

技术发展不顺利，行业应用进展不顺利。

支付+汽车双主业再起航

◆转型升级新能源汽车配件，受益行业高速成长

公司 2015 年完成湖北福田 70%股权收购，并与福田产业投资合作发展新能源专用车业务，规划年产 1.5 万台新能源电动物流车项目一期建设预计将于 2016 年三季度完成建设并投产。公司开发完成汽车总成件计百余套件，成为多家著名汽车客户的一级配套商，新能源车配件占比的上升有力提升了公司的毛利率水平，2015 年上升 0.8%至 12.71%。在政策支持和节能环保等因素的驱动下，新能源汽车行业景气度仍将持续，公司将直接受益。

◆联动优势业务布局完整，市场地位领先

联动优势业务范围涵盖移动信息服务、移动运营商计费结算服务、互联网支付、移动电话支付、银行卡收单、供应链金融、大数据服务及跨境支付等领域。拥有全国范围内从事“互联网支付”、“移动电话支付”、“银行卡收单”三张业务许可牌照。其中公司在第三方移动支付市场排名第五，将显著受益于市场增长，预计未来三年复合增长率在 30%以上。移动信息服务业务随着上海等市场开拓以及联信通业务占比提升有望重迎高增长。“惠商+”O2O 逐步由运营商市场向银行、航空等积分市场拓展，预计稳定之后每年给公司贡献近 4500 万元的收入。大数据业务有丰富的支付数据积累，借助行业高增长势头，预计将有翻倍的增长。

◆拓展区块链技术在金融领域应用可期

联动优势股东李嘉诚基金会与区块链技术公司 Blockstream 的投资者之一维港投资同属李嘉诚旗下，后者领投了 BlockstreamA 轮总计 5500 万美金的融资。Blockstream 是一家由多名比特币工程师创立的加密电子货币及区块链（Blockchain)技术公司，专注于进行加密电子货币创新，以“侧链”技术为核心。侧链可以实现将资产从一个区块链转移到其他区块链，克服了加密电子货币的设计局限性，扩大比特币系统，目前技术尚处于测试阶段。联动优势拥有五大行在内的众多银行客户，而区块链技术重新定义了金融科技内外的生态系统，与相关技术公司合作拓展区块链技术在金融领域应用值得期待。

◆估值与评级

我们预计公司 2016-2018 年实现净利润 3.01 亿元、4.04 亿元、5.02 亿元，增发完成后的 EPS 分别为 0.47 元、0.63 元、0.78 元，6 个月目标价 30.55 元，维持“买入”评级。

◆风险提示：

并购重组进展不顺利，市场竞争加剧。

业绩预测和估值指标

指标	2014	2015	2016E	2017E	2018E
营业收入（百万元）	2,506	2,065	3,233	3,793	4,416
营业收入增长率	-19.70%	-17.60%	56.57%	17.29%	16.44%
净利润（百万元）	30	73	301	404	502
净利润增长率	-49.01%	143.10%	310.86%	34.27%	24.47%
EPS（元）	0.05	0.11	0.47	0.63	0.78
ROE（归属母公司)（摊薄）	2.14%	4.97%	4.24%	5.42%	6.38%
P/E	640	263	64	48	38
P/B	14	13	3	3	2

买入（维持）

当前价/目标价：28.17/30.55 元
目标期限：6 个月

分析师

姜国平 (执业证书编号：S0930514080007)
021-22169167
jianggp@ebscn.com

薛亮 (执业证书编号：S0930515050004)
021-22167311
xueliang@ebscn.com

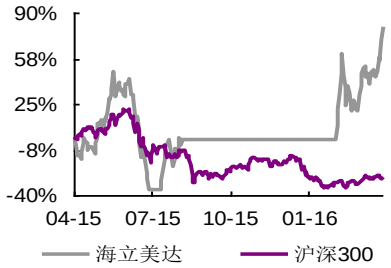
联系人

卫书根
021-22167336
weishugen@ebscn.com

市场数据

总股本(亿股)： 3.01
总市值(亿元)：90.07
一年最低/最高(元)：10.66/38.10
近 3 月换手率：154.65%

股价表现(一年)



收益表现

%	一个月	三个月	十二个月
相对	43.85	79.07	110.49
绝对	50.87	80.25	84.84

相关研报

收购联动优势，支付+汽车双主业再起航 …… 2016-02

2016 年 4 月 17 日

广电运通（002152.SZ） 计算机行业

光大证券 EVERBRIGHT SECURITIES

外延助力 ATM 龙头谋转型

◆国内金融机具龙头，行业维持稳定增长

公司是国内 ATM 龙头，2015 年 ATM 业务实现收入 22.90 亿元，同比增长 13%，市场占有率 26.61%。由于行业竞争加剧单产品价格有一定下调，毛利率由 2014 年的 55%下降为 52%。根据 PBR 发布的《2020 全球 ATM 市场及预测报告》显示，2020 年中国 ATM 机保有量将达到 100 万台，目前安装量累计达到 70 多万台，中国 ATM 市场将进入平稳增长期。同时，公司不断拓展 AFC 产品核心模块应用领域，AFC 产品呈现高速增长态势，2015 年收入同比增长 2 倍达到 7771 万元。清分机全系列产品入围邮政邮储，主流型号入围浦发、华夏、平安总行，VTM 产品新入围浦发银行、华夏银行、中国银行(香港)、永隆银行，在交通银行、广发银行、北银消费公司、土耳其科威特银行实现批量上线应用，行业领先地位优势明显。

◆外延拓展保安押运，金融外包全产业链布局

公司拥有开展金融外包服务子公司 12 家，总计覆盖 90 个城市，已开展外包项目达 193 个，累计承接外包服务设备 7,300 多台。在金融维保领域，公司累计建设服务网点总数达 809 个。在武装押运领域，公司 2015 年完成八家武装押运公司的投资，计划未来五年每年收购 20 家，站到市场三分之一的份额。随着银行出于降低营运成本逐渐将非核心业务外包的趋势，结合公司积累的银行客户资源和国企背景，金融外包服务将实现快速增长。

◆投资神州数码，业务合作可期

截至 2016 年 3 月 21 日收盘公司共持有神州数码 1.11 亿股普通股，占后者已发行普通股股份的 10.09%。一方面，神州数码作为中国最大的整合 IT 服务商，当前港股估值 2016 年仅 17 倍，算上分红，相比 A 股有明显的估值优势。另一方面，神州数码是国内智慧城市建设第一品牌，已经拿下 50 多个城市建设项目；同时在金融服务领域也深耕多年，拥有 60 多家保安押运公司。公司目前是神州数码第一大股东，基于股权基础后续两者进行资源对接和业务合作值得期待。

◆投资建议：

我们预计公司 2016-2018 年 EPS 分别为 0.97、1.11、1.27 元，首次覆盖给予“增持”评级，目标价 30.00 元。

◆风险提示：

金融机具产品毛利率进一步下滑，金融服务业务增长不达预期。

业绩预测和估值指标

指标	2014	2015	2016E	2017E	2018E
营业收入（百万元）	3,152	3,973	5,017	6,538	8,317
营业收入增长率	25.28%	26.05%	26.27%	30.32%	27.21%
净利润（百万元）	807	898	1,052	1,202	1,371
净利润增长率	14.52%	11.27%	17.04%	14.33%	14.05%
EPS（元）	0.75	0.83	0.97	1.11	1.27
ROE（归属母公司）（摊薄）	19.47%	19.92%	12.08%	12.41%	12.68%
P/E	31	28	24	21	18
P/B	6	6	3	3	2

增持（首次）

当前价/目标价：26.90/30.00 元

目标期限：6 个月

分析师

姜国平 (执业证书编号：S0930514080007)
021-22169167
jianggp@ebscn.com

薛亮 (执业证书编号：S0930515050004)
021-22167311
xueliang@ebscn.com

联系人

卫书根
021-22167336
weishugen@ebscn.com

市场数据

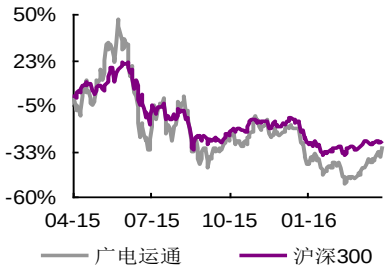
总股本(亿股)： 10.80

总市值(亿元)：251.31

一年最低/最高(元)：18.13/58.00

近 3 月换手率：38.08%

股价表现(一年)



收益表现

%	一个月	三个月	十二个月
相对	28.96	16.45	-3.01
绝对	35.59	17.27	-28.93

2016 年 4 月 17 日

御银股份（002177.SZ） 计算机行业

光大证券 EVERBRIGHT SECURITIES

ATM 受益国产化浪潮，关注新业务进展

◆受益于 ATM 机国产化

公司是国内 ATM 领先企业，2015 年占国内 ATM 机市场 11.74%的份额，位列第四。根据 PBR 发布的《2020 全球 ATM 市场及预测报告》显示，2020 年中国 ATM 机保有量将达到 100 万台，目前安装量累计 70 多万台，尚有一定的增长空间。与此同时，2015 年国产 ATM 机占据 73%的市场份额，相比 2014 年的 60%有了进一步提升。随着国产 ATM 机性能的进一步提升以及相关厂商的本土化优势，ATM 机国产化大势所趋，公司在国内市场份额位居前列，显著受益。

◆参股前海股权交易中心，互联网金融业务值得期待

公司 2015 年出资 2 亿元认购前海股权交易中心新增 7.6%的注册资本，后者是广东省区域性股权交易市场的核心组织机构，注册资本 11.77 亿元，利用互联网平台资源，为广大处于初创和发展阶段、尚未上市的中小微企业提供私募、个性、定制化的金融解决方案。公司参股之后将能够有效推动多方业务形成广泛协同，有利于整合公司自身优势及资源，推动金融资本与实业资本融合发展，延伸市场的价值链，形成新的利润增长点，保证公司发展战略规划的实现。

◆当前股价与员工持股价格持平，具有一定的安全边际

公司前后共推出两期员工持股计划：一期在 2015 年 2 月完成，资金规模约 3200 万，购买成本 8.63 元；二期计划在 2016 年 2 月完成，资金规模约 3000 万，购买均价 7.62 元。两期员工持股计划都由大股东出借 80%的资金，激励对象包括公司管理层和主要业务骨干。公司当前股价基本与两期持股均价持平，具有一定的安全边际。

◆投资建议：

公司在互动易平台上明确表示区块链技术由于最近在互联网金融和支付行业的应用引起广泛关注，目前在组织团队进行研究，希望利用区块链技术在信息安全及身份识别领域的应用机会，提高产品的安全和效率。我们预计公司 2016-2018 年 EPS 分别为 0.17、0.21、0.24 元，首次覆盖给予“增持”评级，目标价 10.50 元。

◆风险提示：

行业竞争加剧带来毛利率下滑的风险，新业务拓展不达预期的风险。

业绩预测和估值指标

指标	2014	2015	2016E	2017E	2018E
营业收入（百万元）	972	1,097	1,262	1,426	1,582
营业收入增长率	14.50%	12.89%	15.00%	13.00%	11.00%
净利润（百万元）	132	69	132	157	180
净利润增长率	6.13%	-47.39%	89.83%	19.27%	14.47%
EPS（元）	0.17	0.09	0.17	0.21	0.24
ROE（归属母公司）（摊薄）	8.20%	4.20%	7.38%	8.09%	8.48%
P/E	51	96	51	43	37
P/B	4	4	4	3	3

增持（首次）

当前价/目标价：8.78/10.50 元

目标期限：6 个月

分析师

姜国平 (执业证书编号：S0930514080007)
021-22169167
jianggp@ebscn.com

薛亮 (执业证书编号：S0930515050004)
021-22167311
xueliang@ebscn.com

联系人

卫书根
021-22167336
weishugen@ebscn.com

市场数据

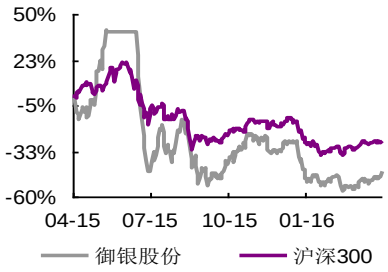
总股本(亿股)： 7.61

总市值(亿元)：66.83

一年最低/最高(元)：6.50/23.18

近 3 月换手率：172.89%

股价表现(一年)



收益表现

%	一个月	三个月	十二个月
相对	22.11	13.89	-16.51
绝对	30.65	17.69	-42.41

分析师声明

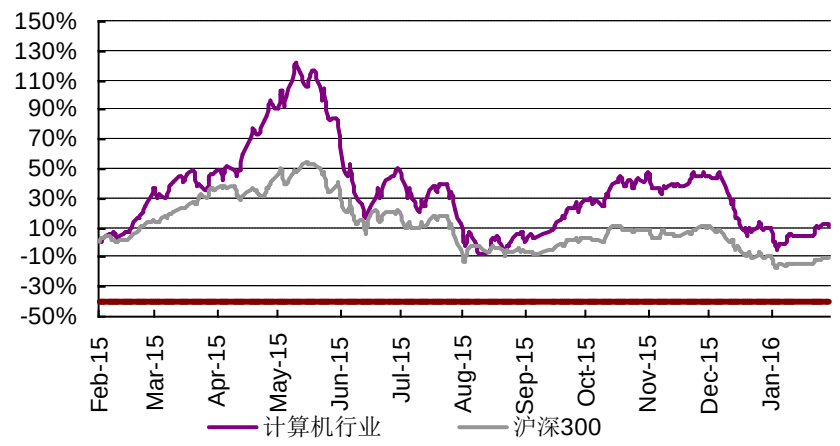
负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及光大证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

分析师介绍

姜国平，复旦大学管理学硕士，中国科学技术大学管理信息系统专业本科。4 年国际 IT 咨询公司工作经验，超过 3 年计算机行业研究经验，14 年加盟光大证券。全面覆盖计算机各子行业。熟悉公司：用友软件、东软集团、卫宁软件、银江股份、易华录、汉得信息、东华软件、广联达、恒生电子、数字政通等。

薛亮，北京邮电大学理学学士，光大证券计算机行业研究员。5 年计算机行业创业经历，主要面向电信、金融行业及政府部门提供软件开发、技术服务；4 年投资银行从业经历，具备丰富的投融资经验；于 2015 年加入光大证券研究所。研究注重框架与逻辑，擅长前瞻性把握行业发展趋势。

投资建议历史表现图



资料来源：光大证券研究所

日期	评级
2015-01-26	买入
2015-01-30	买入
2015-02-01	买入
2015-02-02	买入
2015-03-01	买入
2015-04-26	买入
2015-05-06	买入
2015-05-10	买入
2015-07-19	买入
2015-08-12	买入

买入—	增持—	中性—
减持—	卖出—	

行业及公司评级体系

买入—未来 6-12 个月的投资收益率领先市场基准指数 15%以上；
增持—未来 6-12 个月的投资收益率领先市场基准指数 5%至 15%；
中性—未来 6-12 个月的投资收益率与市场基准指数的变动幅度相差-5%至 5%；
减持—未来 6-12 个月的投资收益率落后市场基准指数 5%至 15%；
卖出—未来 6-12 个月的投资收益率落后市场基准指数 15%以上；
无评级—因无法获取必要的资料，或者公司面临无法预见结果的重大不确定性事件，或者其他原因，致使无法给出明确的投资评级。
市场基准指数为沪深 300 指数。

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

特别声明

光大证券股份有限公司（以下简称“本公司”）创建于 1996 年，系由中国光大（集团）总公司投资控股的全国性综合类股份制证券公司，是中国证监会批准的首批三家创新试点公司之一。公司经营业务许可证编号：z22831000。

公司经营范围：证券经纪；证券投资咨询；与证券交易、证券投资活动有关的财务顾问；证券承销与保荐；证券自营；为期货公司提供中间介绍业务；证券投资基金代销；融资融券业务；中国证监会批准的其他业务。此外，公司还通过全资或控股子公司开展资产管理、直接投资、期货、基金管理以及香港证券业务。

本证券研究报告由光大证券股份有限公司研究所（以下简称“光大证券研究所”）编写，以合法获得的我们相信为可靠、准确、完整的信息为基础，但不保证我们所获得的原始信息以及报告所载信息之准确性和完整性。光大证券研究所可能将不时补充、修订或更新有关信息，但不保证及时发布该等更新。

本报告根据中华人民共和国法律在中华人民共和国境内分发，仅供本公司的客户使用。

本报告中的资料、意见、预测均反映报告初次发布时光大证券研究所的判断，可能需随时进行调整。报告中的信息或所表达的意见不构成任何投资、法律、会计或税务方面的最终操作建议，本公司不就任何人依据报告中的内容而最终操作建议作出任何形式的保证和承诺。

在法律允许的情况下，本公司及其附属机构可能持有报告中提及的公司所发行证券的头寸并进行交易，也可能为这些公司提供或正在争取提供投资银行、财务顾问或金融产品等相关服务。投资者应当充分考虑本公司及本公司附属机构就报告内容可能存在的利益冲突，不应视本报告为作出投资决策的唯一参考因素。

在任何情况下，本报告中的信息或所表达的建议并不构成对任何投资人的投资建议，本公司及其附属机构（包括光大证券研究所）不对投资者买卖有关公司股份而产生的盈亏承担责任。

本公司的销售人员、交易人员和其他专业人员可能会向客户提供与本报告中观点不同的口头或书面评论或交易策略。本公司的资产管理部和投资业务部可能会作出与本报告的推荐不相一致的投资决策。本公司提醒投资者注意并理解投资证券及投资产品存在的风险，在作出投资决策前，建议投资者务必向专业人士咨询并谨慎抉择。

光大证券股份有限公司研究所销售交易总部

上海市新闸路 1508 号静安国际广场 3 楼 邮编 200040

总机：021-22169999 传真：021-22169114、22169134

销售交易总部	姓名	办公电话	手机	电子邮件
上海	严非	021-22169086	13127948482	yanfei@ebscn.com
	周薇薇	021-22169087	13671735383	zhouww1@ebscn.com
	徐又丰	021-22169082	13917191862	xuyf@ebscn.com
	李强	021-22169131	18621590998	liqiang88@ebscn.com
	张弓	021-22169083	13918550549	zhanggong@ebscn.com
	罗德锦	021-22169146	13661875949	luodj@ebscn.com
	叶群	021-22167056	18202166041	yequn@ebscn.com
	黄素青	021-22169130	13162521110	huangsuqing@ebscn.com
	濮维娜	021-22167099	13611990668	puwn@ebscn.com
	计爽	021-22167101	18017184645	jishuang@ebscn.com
	丁梅	021-22167321	13381965696	dingmei@ebscn.com
	邢可	021-22167108	15618296961	xingk@ebscn.com
	陈晨	021-22167330	15000608292	chenchen66@ebscn.com
	吕程	021-22169152	18500502917	lvch@ebscn.com
	王昕宇	021-22169129	15216717824	wangxinyu@ebscn.com
北京	郝辉	010-58452028	13511017986	haohui@ebscn.com
	黄怡	010-58452027	13699271001	huangyi@ebscn.com
	梁晨	010-58452025	13901184256	liangchen@ebscn.com
	刘公直	010-58452029	18610082695	liugongzhi@ebscn.com
	朱林	010-59046212	18611386181	zhulin1@ebscn.com
	杜婧瑶	010-58452038	13910115588	dujy@ebscn.com
	张玮琦	-	18500177850	zhangwq@ebscn.com
深圳	黎晓宇	0755-83553559	13823771340	lixy1@ebscn.com
	李潇	0755-83559378	13631517757	lixiao1@ebscn.com
	张亦潇	0755-23996409	13725559855	zhangyx@ebscn.com
	王渊锋	0755-83551458	18576778603	wangyuanfeng@ebscn.com