国金证券 SINOLINK SECURITIES
证券研究报告

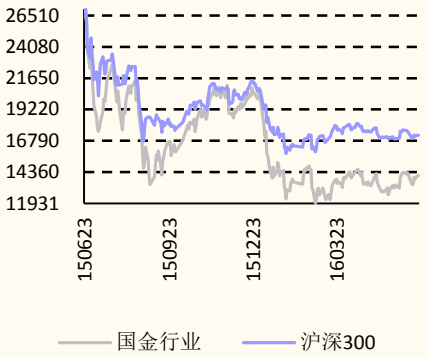
计算机行业 2016 年深度报告

评级：增持　　首次评级　　行业深度研究

长期竞争力评级：高于行业均值

市场数据(人民币)

行业优化平均市盈率	48.21
市场优化平均市盈率	15.85
国金计算机指数	14111.61
沪深 300 指数	3112.67
上证指数	2888.81
深证成指	10221.85
中小板综指	11268.04



相关报告

1.《回归价值，回归商业-国金计算机行业周报 第 11 期》，2016.6.12

2.《科技观察：且看大象如何起舞-计算机行业行业研究周报》，2016.5.30

3.《发改委印发《人工智能三年行动实施方案》，发力人工智能技术提升...》，2016.5.24

4.《政策强推电子病历与分级诊疗，积极布局医疗信息化板块机会-计算...》，2016.5.23

5.《科技巨头观察 2：谷歌开发者大会深度解读，AI 与 VR 成谷歌未来...》，2016.5.20

宁远贵　联系人
(8621)61038200
ningyuangui@gjzq.com.cn

魏立　分析师 SAC 执业编号：S1130516010008
(8621)60230244
weili1@gjzq.com.cn

当金融科技遇到区块链
---世界金融技术体系 500 年后的再重构

行业观点

- **区块链是一种安全存储协议，解决互联网价值传输与信任问题。**区块链是一本全网记录所有发生交易信息的公开账本，在区块链上进行支付时全网计算机共同查询区块链数据，共同验证这笔支付交易是否有效，确认支付后将写入区块链并产生一条不可篡改记录。区块链有去中心化、开放性、自治性、信息不可篡改以及匿名性等特性，通过加密技术与集体维护实现去中心情况下的安全性问题，解决信息互联网的信任问题，解决价值安全传输的痛点。
- **依托区块链构建价值互联网，重塑社会组织与生产方式。**价值互联网由区块链作为底层技术支撑，它实现的不仅仅是人和人的金钱的流动，更是人与人、人设备、设备与设备之间信息的转移与资源的有效分配，就像传统的金钱使得人与人或者公司与公司之间的分工协作成为可能。所以价值互联网以价值的转移为核心组织社会生产活动协调运转，将重塑当前社会组织与生产方式。
- **金融科技变革催生金融体系的变革，价值互联网革命迎来了五百年一次金融体系的变革。**金融的本质是价值流通，相应的金融体系是整个经济的润滑剂，金融科技革命会带来金融体系的变革，金融创新能够推动产业发展。 从 12 世纪威尼斯到 17 世纪以来伦敦与纽约，再到区块链带来金融体系再次变革的当下，金融科技变革带来五百年一次的金融体系变革。在金融体系变革在即的当下，英国已经将区块链上升为国家战略，誓要抢回全球金融中心地位，在人民币国际化的背景下，中国也不会错过这次同步世界的技术变革。
- **技术不断突破，资本不断进入，行业将迎质变**

互联网的发展主要分为网络传输技术与终端技术的发展与普及，随着技术的发展与网络的普及应用逐渐丰富。对比互联网行业的发展，当前区块链还处于早期，由于智能终端与底层传输技术已经成熟，未来价值互联网的发展主要依赖区块链技术的吞吐量、安全性、存储空间需求等性能的提升与优化，随着技术的进步建立在价值互联网上的应用于价值也将呈现爆发式增长。

制约当前已区块链为核心的价值互联网应用发展的阻碍主要有：吞吐量、确认延时、安全性、存储空间需求等问题，从区块链与 IBM OBC 的技术指标来看性能已经得到大幅提升，一方面通过私有链与联盟链提升吞吐量减少延时提升安全性，另一方面通过 POS、DPOS 等共识机制提升系统效率，降低计算资源占用。从以太坊的底层平台推出时间表来看，通过分片与状态通道以及新的共识机制系统性能还能够得到大幅提升，达到“没有限制”的扩展性。区块链技术上的突破与资本不断进入，推动行业迎来质变。

投资建议

- 区块链为价值互联网的发展提出了一个很好的发展方向，同时为各领域应用提供了底层的区块链安全存储系统。我们认为在价值互联网各领域的需求拉动下，底层协议性能将得到逐步优化，将会涌现出更多区块链底层平台与应用，行业发展进程将远超市场预期。建议关注：海立美达、飞天诚信、四方精创、赢时胜、金证股份、恒生电子、御银股份以及广电运通。

风险提示

- 区块链技术发展不达预期，区块链应用推广进程不达预期。

内容目录

前言：世界金融技术体系 500 年后的再重构 5
1、从比特币说起 5
1.1、比特币简介 5
1.2、比特币底层加密算法原理 6
1.3、比特币交易单产生与验证原理 6
1.4、区块链生成与验证 7
1.5、比特币优缺点 9
1.6、比特币底层技术区块链逐渐得到广泛应用 9
2、区块链是价值互联网的核心，颠覆现有生产方式 11
2.1、区块链解决去中心的信任问题 11
2.2、基于区块链构建价值互联网 12
2.3、五百年一次金融体系的变革，中国不会缺席 15
3、区块链三个发展阶段，应用领域逐渐丰富 16
3.1、区块链 1.0，可编程货币 16
3.2、区块链 2.0 ，可编程金融 17
3.3、区块链 3.0，可编程社会 21
4、区块链应用与相应初创公司介绍 24
4.1、锐波科技 24
4.2、纳斯达克 linq 25
4.3、以太坊（Ethereum） 25
4.4、GetGems 26
4.5、OpenBazaar 27
4.6、小蚁(AntShares) 28
4.7、Factom 28
4.8、其他应用 29
5、技术突破超预期，巨头大幅投入，新贵不断崛起 30
5.1、技术不断获得突破 30
5.2、各国政府积极表态，抢占价值互联网技术制高点 31
5.3、巨头与新贵共舞 32
6、标的推荐 34
赢时胜 34
恒生电子 34
海立美达 34
四方精创 35
飞天诚信 35
御银股份 35
长亮科技 35

广电运通 36
金证股份 36

图表目录

图表 1：五百年一次金融体系的变革 5
图表 2：区块链带来互联网金融 2.0 5
图表 3：比特币价格走势 5
图表 4：公钥/私钥加密原理 6
图表 5：哈希散列原理图 6
图表 6：比特币交易单内容 7
图表 7：比特币交易流程与原理 7
图表 8：比特币交易流程 7
图表 9：区块链简图 8
图表 10：区块生产与验证流程 8
图表 11：比特币区块内容 9
图表 12：比特币底层区块链架构图 10
图表 13：区块链本质是分布式安全存储与验证协议 11
图表 14：数据库技术发展 11
图表 15：区块链去中心化 12
图表 16：区块链解决信任问题 12
图表 17：互联网架构图 13
图表 18：区块链分层架构 13
图表 19：区块链分层架构 14
图表 20：科技革命发展路径 14
图表 21：五百年一次金融体系的变革 15
图表 22：区块链发展三个阶段 16
图表 23：货币是协调社会生产活动与资源分配的纽带 16
图表 24：电子货币市值排名 17
图表 25：区块链应用领域 18
图表 26：智能合约 18
图表 27：智能合约 19
图表 28：基于区块链众筹架构 19
图表 29：区块链在 P2P 交易中的应用架构 20
图表 30：区块链在保险行业应用 20
图表 31：区块链带来物联网新革命 21
图表 32：区块链在 医疗行业应用 22
图表 33：区块链应用路径 22
图表 34：基于区块链物流应用架构 22

图表 35：区块链应用领域与相应公司 24
图表 36：锐波科技清算原理图 24
图表 37：纳斯达克 linq 25
图表 38：以太坊（Ethereum） 26
图表 39：GetGems 界面 27
图表 40：OpenBazaar 界面 27
图表 41：小蚁(AntShares) 28
图表 42：Factom 系统架构 29
图表 43：区块链其他领域应用 29
图表 44：各种共享机制优缺点 30
图表 45：公有链 、私有连、联盟链优缺点介绍 30
图表 46：区块链平台参数对比 31
图表 47：以太坊平台推出时间表 31
图表 48：各国政府对区块链态度 31
图表 49：R3 成员 32
图表 50：中国分布式总账基础协议联盟成员 32
图表 51：区块链领域投资规模 33
图表 52：区块链领域创业公司 33

前言：世界金融技术体系 500 年后的再重构

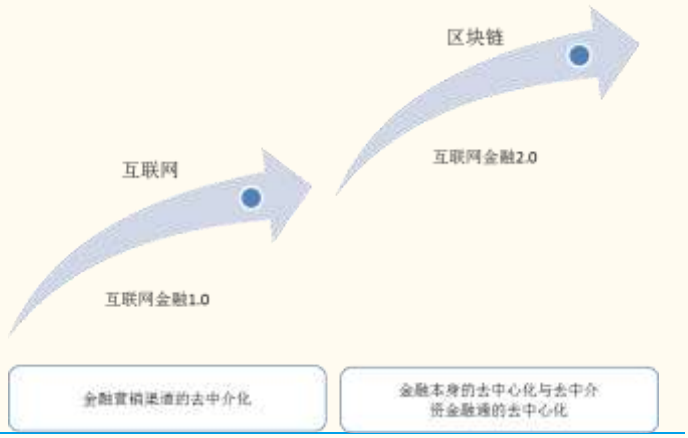
- 金融科技变革催生金融体系的变革，价值互联网革命迎来了五百年一次金融体系的变革。金融的本质是价值流通，相应的金融体系是整个经济的润滑剂，金融科技革命会带来金融体系的变革，金融创新能够推动产业发展。从 12 世纪威尼斯到 17 世纪以来伦敦与纽约，再到区块链带来金融体系再次变革的当下，金融科技变革带来五百年一次的金融体系变革。在金融体系变革在即的当下，英国已经将区块链上升为国家战略，誓要抢回全球金融中心地位，在人民币国际化的背景下，中国也不会错过这次同步世界的技术变革。

图表 1：五百年一次金融体系的变革

时间	12世纪	17世纪	21世纪
金融中心	威尼斯	伦敦、纽约	？
产业变革	城市、商贸	工业革命	信息革命
金融体系变革	资金清算体系、铸币制度建立（纯银铸币，“格罗索”，中世纪的美元’）	国债、银行、券商体系建立	基于区块链交易体系

来源：国金证券研究所

图表 2：区块链带来互联网金融 2.0



来源：国金证券研究所

1、从比特币说起

1.1、比特币简介

- 比特币是一种电子货币。2008 年一个叫做中本聪的组织在一片论文中提出了一种电子货币的设计思路与细节，随后在 2009 年比特币客户端和首批比特币发布，比特币网络正式上线，2010 年比特币首次公开交易，11 月市值超过 100 万美元，此后比特币价格一路飙升，13 年 末已经比特币价格突破 900 美元，随后出现暴跌，当前比特币价格已突破 600 美元。

图表 3：比特币价格走势

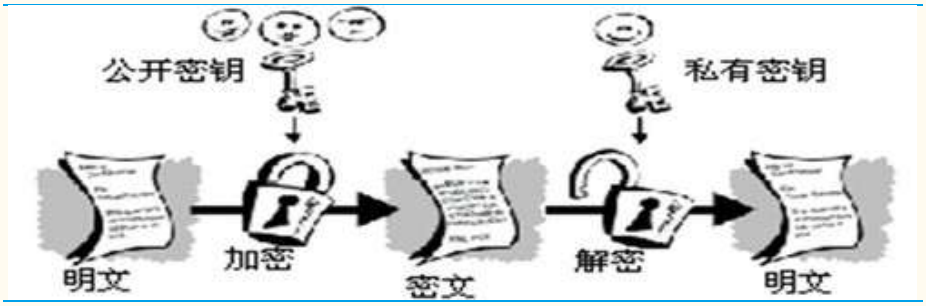
来源：互联网 国金证券研究所

- 比特币是一种利用加密技术来实现独立于中央银行之外，协议地发行和验证支付有效性的电子货币和在线支付系统。货币的支付不通过中心机构，支付记录会向全网节点发送并记录，通过全网节点的计算验证其有效性，货币的发行是对各节点运算工作的奖励，通过这种方式为用户提供计算机算力来核对保障比特币支付，随着比特币总量的增加，新币制造的速度减慢，直到 2140 年达到 2100 万个的总量上限。

1.2、比特币底层加密算法原理

- **公钥（Public Key）与私钥（Private Key）**是通过一种算法得到的一个密钥对，公钥是密钥对中公开的部分，私钥则是非公开的部分。需要给某人发送信息只需要用其公钥加密后广播出去，因为只有相应的私钥才能解密获得信息，某人需要证明该信息是出自自己，用私钥加密，其他人使用此人公钥能够解密即能够证明该信息出自此人。比特币系统中公钥相当于账号，私钥相当于密码。

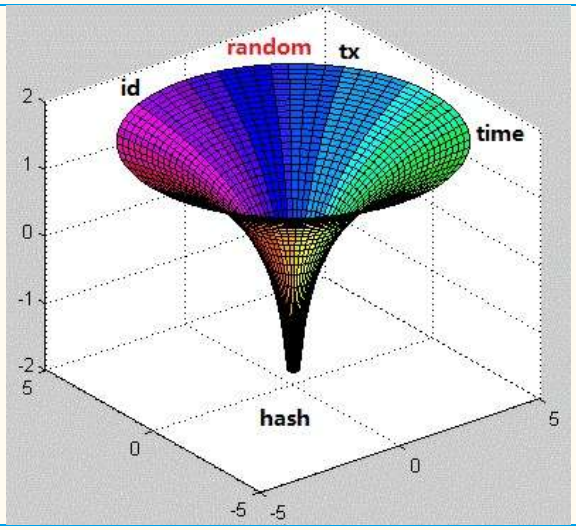
图表 4：公钥/私钥加密原理



来源：公开资料 国金证券研究所

- **哈希散列**能够将任意长度的输入，通过散列算法变换成固定长度的输出，该输出就是散列值。输入值的变化能够使得散列值发生变化，散列值的空间远小于输入的空间，所以从散列值不能够推出输入值。哈希散列主要用来压缩信息空间，另一方面验证收入准确性。

图表 5：哈希散列原理图

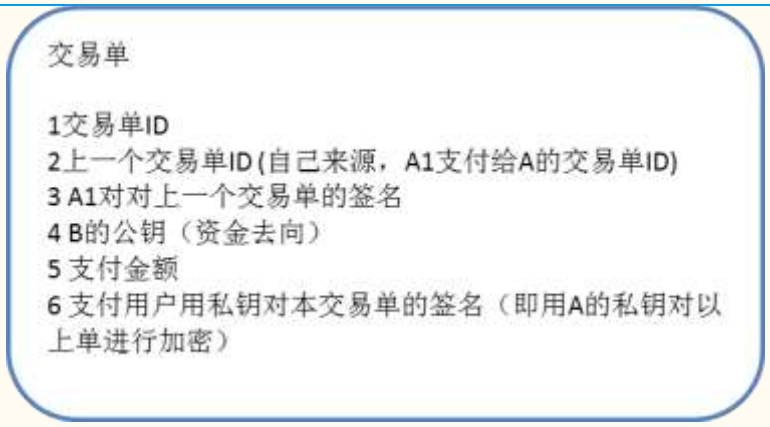


来源：公开资料 国金证券研究所

1.3、比特币交易单产生与验证原理

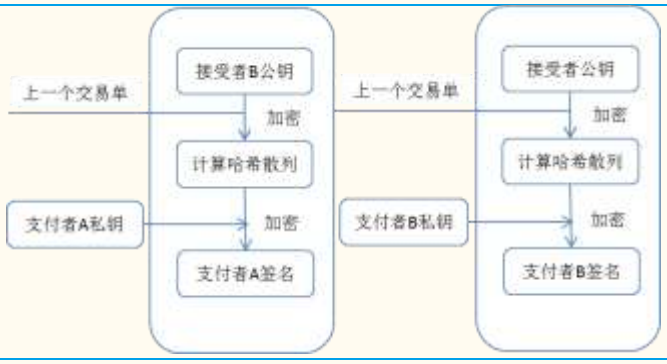
- 假设 A 要给 B 支付一笔钱，这笔钱是 A1 原来支付给 A 的，首先 A 生成一张交易单，其中包括交易单 ID、该资金的上一笔交易单 ID（资金来源）、A1 对上一张交易单的签名、接受者的公钥（B 的公钥）、支付数额以及 A 用私钥对本交易单的签名。

图表 6：比特币交易单内容



来源：国金证券研究所

图表 7：比特币交易流程与原理



来源：国金证券研究所

- A 生成交易单向全网节点广播，B 收到交易单后用 A 的公钥解密，能够确认是 A 付的钱，并获得散列值 X，收款人利用自己的公钥与上一个交易单的散列值 Y，如果 X=Y 即说明交易单有效。

图表 8：比特币交易流程

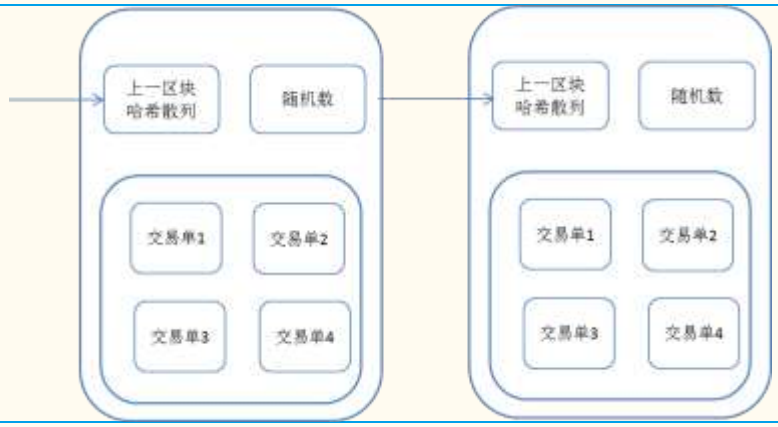
来源：国金证券研究所

1.4、区块链生成与验证

- 区块是包含多个交易单以及一些验证信息的交易单包，通过记录上一区块的散列值挨个相连形成区块链，并将其储存在全网各个节点以增强其安全性，区块主要是用来记录历史交易，以及验证交易有效性的存储机制。

- 全网节点计算好上一个区块，接着不断接收发出的交易单，生成随机数后打包上一区块哈希散列、各交易单数据以及生成的随机数后生成哈希散列值，通过改变随机数使得生成的散列值满足某一条件（前 10 位为 0）,即生成的区块有效，向全网广播，等待验证。

图表 9：区块链简图



来源：国金证券研究所

图表 10：区块生产与验证流程

来源：国金证券研究所

- 区块信息主要有交易单信息以及验证信息，验证信息包括区块序列号（第几个区块）、时间戳（生成区块的时间）、上一区块的哈希值、本区块交易信息哈希值以及随机数。

图表 11：比特币区块内容

	A	B
1	区块序号：	#388388
2	时间戳：	2015-12-14 18:00:59
3	上一区块HASH：	000000000000000000cdcdc57154cf349fa8ad24831336abe583df544d59e196
4	本区块HASH：	00000000000000000012344120eba5bb76d4097087fe82c69117949c9d800ced4
5	随机数：	1796740019
6	交易列表：	新生块奖励25BTC+0.14002479 BTC手续费 -> 1PE7LXcntsLvavM2KXpJGNu51UbDhC3u63
7		1Gt9XeDYxLhWwMJRBXjAcWCPwEvgoR2tbY -> 1NKQ7bP4UdPoUc8zk4Zduw9Jep1Biqm55P 100 BTC
8		-> 13qZwTHweu6DcdMHs1tHrKM6Eb1X8phc9T 126.99997209 BTC

来源：公开资料 国金证券研究所

1.5、比特币优缺点

- 比特币作为一种新兴的电子货币主要有：交易成本低、安全透明、无通胀等优点。比特币的交易无需第三方，采用点对点网络结算，去中心化使得交易成本极低。系统通过时间戳阻止对历史数据的篡改，通过全网节点参与加密计算来提升当前交易的安全性，通过一系列机制解决了“双花问题”“拜占庭将军”大大提升了电子货币系统的安全性。此外比特币系统的设计类似黄金供应，其上限数量为 2100 万个，能够防止央行滥发导致的通胀。

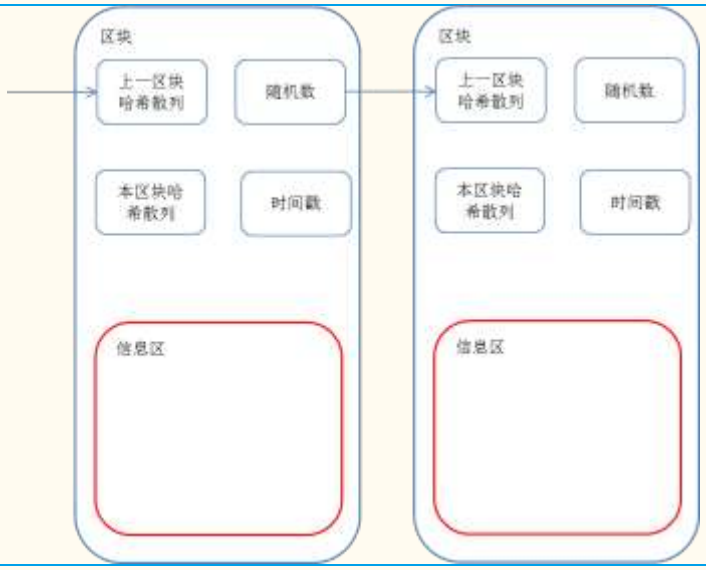
- 同样比特币也存在诸多缺点：价格波动剧烈、吞吐量有限、支付确认延时长、计算资源浪费以及存储容量需求大等。1 吞吐量有限，比特币目前每秒只能处理 7 比交易，与 VISA 每秒处理 2000 笔交易相去甚远，尤其在比特币广泛普及以后吞吐量问题更加严重。2 价格波动大，比特币价格从 11 年 1 美元飙升到 13 年 11 月 600 美元价格，此后大幅下跌，近期有大幅上涨达到 600 美金。剧烈的波动使得资产价值波动性加大，用户使用意愿下降。3 延时，每个区块需要 10 分钟才能验证确认，意味着至少需要 10 分钟才能确认交易，而 VISA 最多只需要 1 秒。4 储存容量，比特币区块链大小是 25G， 这需要至少一天时间下载，如果吞吐量达到 VISA 水平，存储需求每年增长将达 1.4PB/年。 5 资源浪费，为了区中心并且提升安全性，需要全网同时验证区块真实性，这使得每天计算资源的浪费可能达到几千万美元。

1.6、比特币底层技术区块链逐渐得到广泛应用

- 由于比特币为代表的加密电子货币存在诸多问题，还只能作为当前货币体系的有效补充，主要应用在国际支付与汇兑领域，由于各国中央银行的强中心地位短期区块链的电子货币还无法普及，但是比特币的底层技术与协议能够应用到金融交易、智能合约以及社会管理等其他领域中，为价值互联网指明了方向。比特币底层区块链技术能够为去中心话的价值传递提供安全保障，为社会生产活动的自我组织提供了底层技术与协议的借鉴，意义重大。

- 区块链本质上是通过分布式存储与全网验证实现安全信息存储的底层协议，区块中的信息除了包头的验证信息，信息区中的信息可以是交易单也可以是其他信息，根据应用需求储存相应的信息。

图表 12：比特币底层区块链架构图

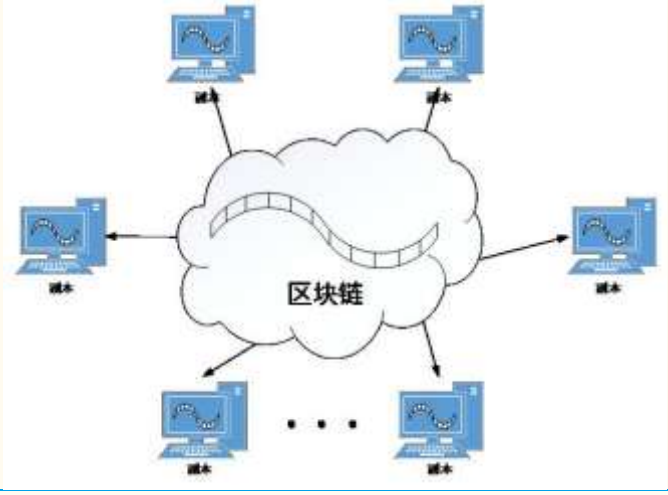


来源：国金证券研究所

2、区块链是价值互联网的核心，颠覆现有生产方式

- 区块链是一本全网记录所有发生交易信息的公开账本，它是一种实时记录全部交易的去中心化公开数据库，在区块链上进行支付时全网计算机共同查询区块链数据，共同验证这笔支付交易是否有效，确认支付后将写入区块链并产生一条不可篡改记录。区块链有去中心化、开放性、自治性、信息不可篡改以及匿名性等特性，是价值互联网的底层存储与传输协议。

图表 13：区块链本质是分布式安全存储与验证协议



来源：公开资料，国金证券研究所

- 随着信息化与互联网的发展，数据种类的正发生变化，从最初的关系数据到大数据，再到当前的安全数据。相应的数据库技术也在快速发展，从最初的关系型数据库，到 Web2.0 与大数据兴起后的非关系型数据库，再到当前价值互联网底层的区块链。区块链本质上是价值互联网底层的存储协议，简单来说可以理解成一个通过分布式存储与验证保证存储信息准确性与安全性的数据库。

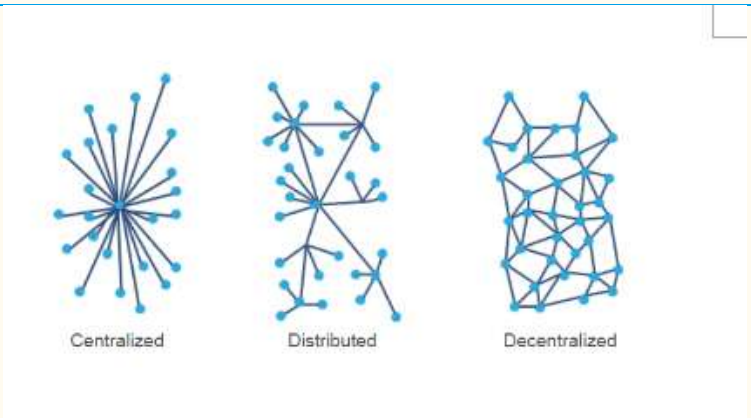
图表 14：数据库技术发展

来源：公开资料，国金证券研究所

2.1、区块链解决去中心的信任问题

- **去中心化。**区块链利用加密技术与全网验证实现去中心化，首先使得交易成本下降，收益在参与方之间分配，而不是中心占据绝大多数收益，其次使得社会组织活动更自由，而不是由中心制定规则，在自组织环境下将会激发创新。

图表 15：区块链去中心化



来源：公开资料，国金证券研究所

- **安全性。**区块链利用时间戳解决了篡改历史信息的问题，其次传输加密使得通信安全性增强，全网验证使得篡改当前信息难度很大，在系统计算资源达到一定程度几乎不可能能够伪造信息。区块链采用时间序列与全网节点集体维护来保证存储信息的不可篡改，保证信息的安全性，从而保证互联网上的价值安全传输，解决信任问题。
- **可编程。**区块链提供灵活的脚本语言，支持用户创建高级应用，满足系统完成去中心与自动化应用。

区块链通过加密技术与集体维护实现去中心的情况下的安全性问题，解决了信息互联网的信任问题，解决价值安全传输的痛点。

图表 16：区块链解决信任问题

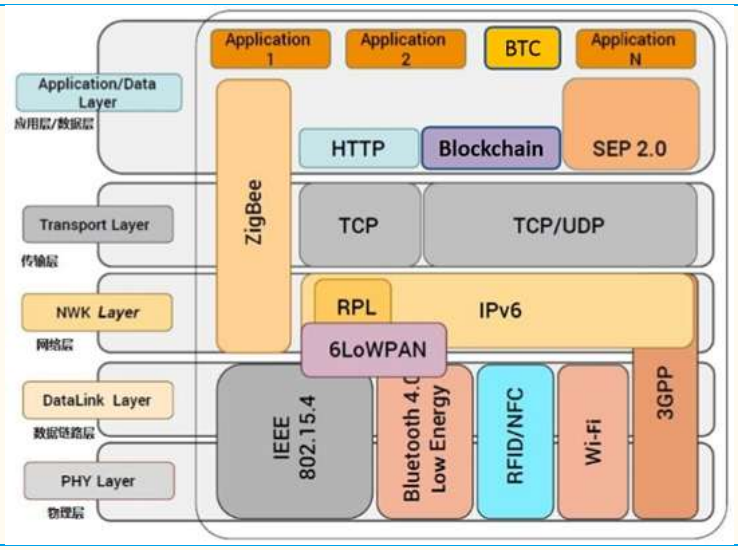
来源：国金证券研究所

2.2、基于区块链构建价值互联网

- 我们将互联网分为五层依次为：物理层、数据链路层、网络层、传输层以及应用层。第一层是物理层，由通信、电缆、光纤、WiFi、3G 等通信网络构成。第二层是数据链路层， 它是各种传输介质上的传输协议。第三层叫作网络层，即通常所讲到的 IP 网络，相当于通过标记数据包的传输地址，借助路由寻找将数据包送到目标地址的路径。第四层叫作传输层。验证协议保证数据报能够完整传输。最上层是应用层，是具体的应用的数据传输协议，例如 FTP、SMTP 以及 HTTP 协议，HTTP 是互联网应用层中 最重要的应用协议，我们依据 HTTP 协议才能解决信息的点对点传播。

- 区块链本质是一个信息安全存储协议，是类似于信息互联网上的应用层协议，通过分布式存储与全网验证保证信息准确性与安全性，解决信息互联网上的信任问题。

图表 17：互联网架构图



来源：公开资料，国金证券研究所

- 在互联网这样一个大的模型中，区块链是在应用层里面的一个价值点对点传输与存储的协议，它与 HTTP 等协议一样完成某些数据在互联网上的传输。它的意义或者价值能够与信息互联网中 HTTP 协议的价值相媲美，没有 HTTP 的协议，我们的网站互相间是找不到的；没有区块链这样一个协议，你要想在没有任何中介帮助的情况下，点对点地在互联网上完成价值传输，几乎也是不可能的，在没有中心或者中介的验证下，无法对传输价值数据有效性的验证。

图表 18：区块链分层架构

来源：国金证券研究所

- TCP/IP 协议之上我们可以吧区块链分为三层，依次分数据与技术层、验证与激励层以及应用层，底层数据与技术层包括密码技术与分布式存储，当前区块链技术主要应用非对称加密以及哈希散列，随着密码技术的发展可能会应用其他的技术，区块链通过分布式存储增加系统安全性，但同时存储与通信瓶颈对系统性能起到了制约影响。验证与激励层包括对于区块生成以及交易信息的验证，以及提供计算资源的奖励，是整个系统的底层核心，也是未来区块链技术不断改进不断发展的领域。上层是应用，涉及货币、金融、以及各行业的资源配置等应用，就像互联网的发展一样先从某些领域突破，出现拓展到各领域。

图表 19：区块链分层架构

来源：公开资料，国金证券研究所

- 互联网创新逐渐深化。从最初的 PC 单机解决逻辑计算自动化，到 00 年的 PC 互联网实现信息链接，到 10 年移动互联网继续深化信息链接场景，再到当前的虚拟现实解决真实场景的连接，每一次互联网的每一次变革与深化都会带来市场的爆发式增长。
- 价值互联网由区块链作为底层技术支撑，它实现的不仅仅是人和人之间的金钱的流动，更是人与人、人设备、设备与设备之间信息的转移与资源的有效分配，就像传统的金钱使得人与人或者公司与公司之间的分工协作成为可能。所以价值互联网是以区块链作为底层技术支撑，以价值的转移为核心的组织社会生产活动的网络。

图表 20：科技革命发展路径

来源：国金证券研究所

2.3、五百年一次金融体系的变革，中国不会缺席

- 金融的本质是价值流通，相应的金融体系是整个经济的润滑剂，产业与金融科技的变革会带来金融体系的变革，金融创新能够推动产业发展。从 12 世纪威尼斯到 17 世纪以来伦敦与纽约，再到区块链带来金融体系再次变革的当下，这一次是信息革命在呼唤五百年一次金融体系的变革。
- 12 世纪之前欧洲还处在自给自足的农业经济时代，日常交易主要通过物物交换达成。13 世纪开始随着城市的形成，商品贸易活动逐渐集中繁荣，催生了货币体系的构建。此后威尼斯建立的资金清算所，使得地区硬币运输减少交易成本下降，同时威尼斯开始采用新的大面额的纯银铸币，成为商业中优先使用的货币，它们很快就为货品供应商和市场所接受，被看作是‘中世纪的美元’，成为货币流通使用的标准。城市与商贸的繁荣催生了以货币为核心的金融体系的建立，同时货币与支付的标准化推动了威尼斯商贸业的繁荣。
- 18 世纪 60 年代英国爆发的第一次产业革命，使得其生产能力发生了质的飞跃，生产力的大发展造成了资本投入的巨大缺口。债券、银行以及券商体系实现了全国性的资金融通，保证了工业大发展的资金需求，是英国工业革命后成为世界工厂的重要保障，此后英国在长达百余年的时间里成为工业生产和世界贸易的第一大国。
- **所以我们认为产业与金融科技变革带来资金融通方式的变化，金融体系的重塑推动产业进一步的发展。**
- 当前信息技术的革命颠覆传统各行业的生产方式，行业的去中心化降低了信息传递的成本。然而信息流的去中心化与资金流的中心化的不匹配推动当前金融体系的变革，区块链技术为本轮金融体系的历史性变革提供了技术与安全保障。
- 所以我们认为产业上的变革提出了金融体系变革的要求，区块链技术的发展提供了有效的支持。在金融体系变革在即的当下，英国已经将区块链上升为国家战略，誓要抢回全球金融中心地位，在人民币国际化的背景下，中国也不会错过这次同步世界的技术变革。

图表 21：五百年一次金融体系的变革

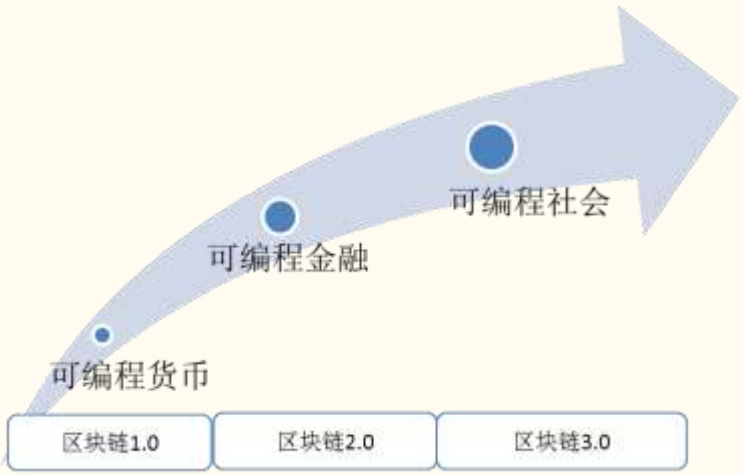
时间	12世纪	17世纪	21世纪
金融中心	威尼斯	伦敦、纽约	?
产业变革	城市、商贸	工业革命	信息革命
金融体系变革	资金清算体系、铸币制度建立（纯银铸币，“格罗索”，中世纪的美元’）	国债、银行、券商体系建立	基于区块链交易体系

来源：国金证券研究所

3、区块链三个发展阶段，应用领域逐渐丰富

■ 区块链的应用可大致分为三个阶段，区块链 1.0、区块链 2.0 以及区块链 3.0。其中区块链 1.0 是在货币领域的应用，实现货币的发行、支付以及汇兑的去中心化，以降低国际货币结算成本。区块链 2.0 是在金融领域交易与合约的的应用，应用领域涵盖股票、债券、期货、贷款、按揭、产权、智能资产以及智能合约。区块链 3.0 是在金融以外的领域的应用，实现相应领域社会活动的自我资源协调与分配。

图表 22：区块链发展三个阶段



来源：自动化学报，国金证券研究所

3.1、区块链 1.0，可编程货币

■ 货币所代表的金钱与利益是协调当前社会生产活动与资源分配的纽带，使得人与公司的生产得以有序运转，所以货币是整个社会生产生活的纽带与润滑剂，是社会价值的核心。

图表 23：货币是协调社会生产活动与资源分配的纽带

来源：公开资料，国金证券研究所

■ 当前整个国际货币体系是一个多中心与多中介的体系，跨国货币的计算成本居高不下，同一国家不同银行间的结算成本也有待下调。高盛此前预测，商业领域中支票支付仍然至少占 50%。以每张支票约 8 美元的成本，这还

不包括人为错误和欺诈损失的成本，传统支付系统使得全球企业每年要耗费 5500 亿美元的额外费用。

- 货币体系多中心与多中介抬高了交易成本，基于区块链的电子加密货币能够大幅降低跨国支付的成本，应用前景广阔。由于基于区块链的金融资产的交易、合约的执行以及社会资源的分配均涉及货币，所以区块链在货币领域的应用也是区块链技术向其他领域应用的基础。
- 当前电子加密货币种类较多，市值排名前三位是比特币、瑞波币以及以太币，从各虚拟货币的市值来看比特币依然是规模最大的虚拟货币，紧随其后的是瑞波币与以太坊，瑞波币致力于服务国际汇兑降低汇兑成本，有较广泛的应用。以太坊内置图灵完备的编程序语言，将其作为协议层内置在以太坊的区块链中，可以让开发者和投资者使用。这个系统被认为能够在企业和普通人构建自己的自治组织，智能合约和应用，同时 R3 CEV，这个由全球最大的 42 家银行支持的区块链基础设施项目，宣布将会使用以太坊和微软 Azure，极大地推动了以太坊的发展。

图表 24：电子货币市值排名

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)
1	Bitcoin	$ 11,846,843,099	$ 755.85	15,673,475 BTC	$ 245,021,000	2.03 %
2	Ethereum	$ 888,283,109	$ 10.95	81,157,321 ETH	$ 135,080,000	-26.61 %
3	Litecoin	$ 257,683,115	$ 5.57	46,287,026 LTC	$ 6,892,790	0.47 %
4	Ripple	$ 230,634,324	$ 0.006569	35,108,326,973 XRP *	$ 1,343,980	-1.78 %
5	The DAO	$ 84,603,531	$ 0.072140	1,172,775,159 DAO *	$ 13,443,500	-31.80 %
6	Dash	$ 53,088,093	$ 8.13	6,530,696 DASH	$ 512,617	-1.72 %

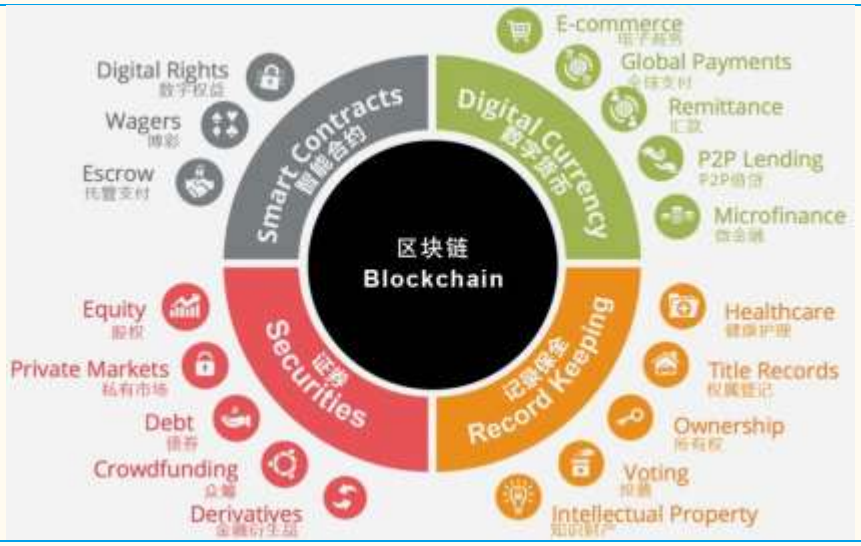
来源：互联网，国金证券研究所

- **电子货币监管严格，实现单点突破局部应用。**由于国家中央银行或者法律要求货币必须由中央银行发行，掌握货币发行权能够行驶国家货币政策调控，所以多数国家完全禁止比特币为代表的加密电子货币，同时也有像德国、法国、韩国以及泰国持观望态度，只有英国将比特币视作货币，美国国税局将其视作资产，其他机构将其视作货币来监管。
- **由于货币的发型与监管涉及国家货币政策的制定与调控，所以很难寄希望于国家政策的松绑，我们认为加密电子货币将会在跨国支付以及区块链其他应用等局部领域率先应用。**

3.2、区块链 2.0，可编程金融

- 价值的交换除了在货币方面的应用，在金融的其他领域尤其是中心与中介使得交易成本大幅提升的领域应用较广泛，包括股票、债券交易、股权众筹以及合约的签订与执行。

图表 25：区块链应用领域



来源：公开资料，国金证券研究所

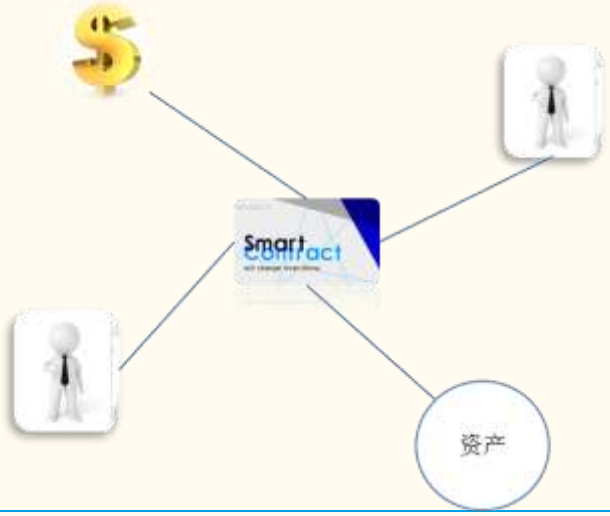
- **智能资产（资产交易）。**区块链可用于任何资产注册、存储和交易，包括金融、经济和货币各个领域，可以是金融资产（如股票、期货、票据）也可以是实物资产（商品、艺术品等）。任何资产可以在区块链上被注册，所有权被任何控制了私钥的人所控制，所有者能通过转移私钥完成出售资产行为。智能资产即通过区块链来控制其所有权通过智能合约来自动执行资产的而交易，比如智能合约能够。
- **智能合约。**合约是参与方为执行某任务事先规定的各方义务与责任的约定，智能合约是能够自动执行合约条款的计算机程序。智能合约早就被提出但是“实现智能合约的一大障碍是现在计算机程序不能真正地触发支付，智能合约能够与区块链电子货币进行交互，从而控制资产的支付与交易，使得智能合约执行成为可能。

图表 26：智能合约

来源：公开资料，国金证券研究所

- 智能合约意味着区块链交易不止简单的买卖，将会有更广泛的指令嵌入到区块链中，一旦条件符合即执行指令进行资产的交易与流转。传统的合约有可能被参与方违约，区块链无需信任对方，它由代码对资产进行自动执行，由于涉及的资产已在区块链上注册，系统可以直接控制资产的划转，有效解决了参与方违约与信任的问题。区块链中，只有合约双方能动用资金；一旦合约确定了，其中的资金就由区块链按照合约条款来分配，并且只有合约到期才可以使用这笔资金。

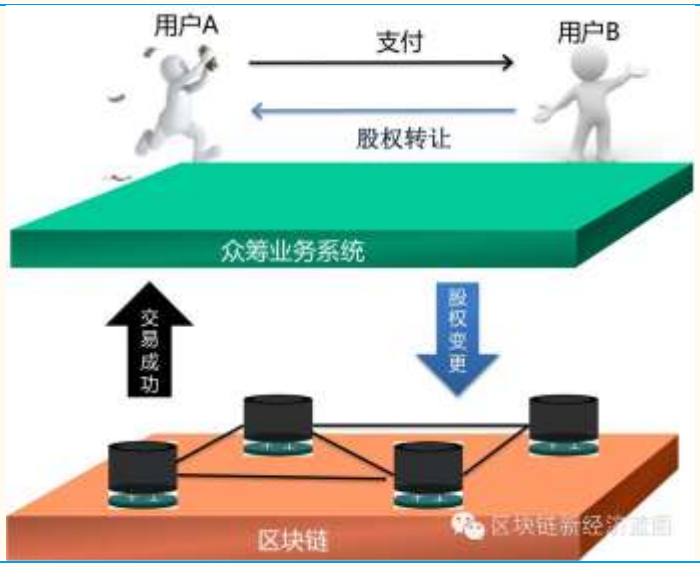
图表 27：智能合约



来源：国金证券研究所

- 社会活动主要就是生产与消费，两大环节是通过合约与交易协调进行的，所以保障合约能够履行是经济正常运行的必要条件。银行、券商、律所等中介机构在促成交易的同时也增加了社会的成本，在价值互联网普及的背景下，现有银行、券商以及律所的运营模式也将发生颠覆性的变革。
- **股权众筹**为创业者提供资金需求，为普通投资者参与到早起股权投资提供机会，满足了普通投资这的资产配置需求，然而对于融资企业合法性、资质以及权属状况需要中筹平台进行核查与增信。对于股权众筹市场，股权流通能够增强市场流动性，激发市场活跃度，但是场外股权交易，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。
- 创业公司的信用风险催生了中筹平台等中介的兴起，进而推高了交易成本，区块链技术可以降低交易的信用风险，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。

图表 28：基于区块链众筹架构



来源：万象区块链实验室，国金证券研究所

- **票据等资产 P2P 交易。**前期农行北京分行保险柜中票据被换成了报纸，消息一出震惊全国，当前市场上除了一票多卖这样的票据违规交易问题外，

票据业务领域还存在着假票、克隆票、变造票等现象。基于区块链上的P2P 票据交易，首先票据的发型需要在区块链上进行登记，所有信息不可篡改，有效杜绝了票据的造价、一票多卖等违规问题，解决了票据交易市场缺乏信任的问题，大大降低交易成本。

图表 29：区块链在 P2P 交易中的应用架构

来源：复杂美区块链研究中心，国金证券研究所

- **审计。**信任是经济的基础，但建立信任需要投入大量的人力资源进行审计和记录核查，从而降低了生产效率。利用区块链所有参与人与公司的数据更新都会被记录到区块链上，这帮助审计师对企业审计中对企业资金流、信息流的审核。由于区块链的不可篡改性保证了信息的准确性，解决了原有人力确认信息准确性的问题，大大降低了升级成本。德勤在经过一年的研发后推出了“一站式区块链软件平台”Rubix，此外普华永道也宣布进军区块链行业。
- **保险。**互助是保险最初的精神，但由于所有人参与的写作保费与损失的计算困难较大，所及就产生了中心化得保险机构。区块链的去中心化、安全性以及可编程很好地解决了保险行业去中心的问题，回归保险本质。用户参与保险社区没有门槛，在没有人生病的情况下，大家都不需要交任何费用，仅仅当有人生病的时候， 每个参与的人才会缴纳费用，费用的计算与支付借助脚本制动执行。

图表 30：区块链在保险行业应用

来源：公开资料，国金证券研究所

3.3、区块链 3.0，可编程社会

- 区块链不仅仅能够重塑各类货币市场、支付系统、金融服务，它能够从根本上成为让组织活动形态减少摩擦并且提高效率。之所以能够实现区中心化，是因为它底层网络有足够的流动性将所以参与者连接在一起，实现资源的配置，以及物理资源与人力资源的分配。区块链能够极大地促进过去由人来完成的各种协调工作，颠覆现有的人与人、人机价值交互方式，使得参与方能够获得更大的自由度、更加平等和更多的授权。
- **区块链政府。**区块链还能够用来提供那些现在国家所提供的传统服务，以区中心化、低成本以及个性化的方式提供公共服务。甚至在极端情况下把国家放在区块链上，提供一个无国家的去中心化的选择以区块链作为基础的治理服务,，包括 ID 系统、争端解决、投票、国民收入分配、登记法律文件。
- **物联网。**当前互联网基本是基于中心化得连接架构，当智能终端数量大幅增长时，中心系统的压力加大，所需的通信传输贷款也将倍增，延时也相应边长。有预测到 2020 年物联网将带来 260 亿个设备，届时现有中心化架构很难满足大量终端交互的需求 。正如基于金钱的经济系统能够使得社会资源更好地协调分配，基于机器的系统也能够借助一个去中心化的支付与验证系统实现资源的有效配置。
- 区块链技术可以使智能设备变作独立代理，自动执行各种转账。设想下一台自动售货机不仅实时监控汇报其仓库情况，并且可以从不同分销商处招标按价高者售，还可以在新品到库时自动付款（当然新品是根据客户购买历史采购）。或者一整套智能家居设备，如洗衣机，洗碗机，吸尘器根据时间及将电力损耗降至最低为目的相互间自动排序运行。或者一台车可自行检测，安排保养并付款。

图表 31：区块链带来物联网新革命

来源：互联网，国金证券研究所

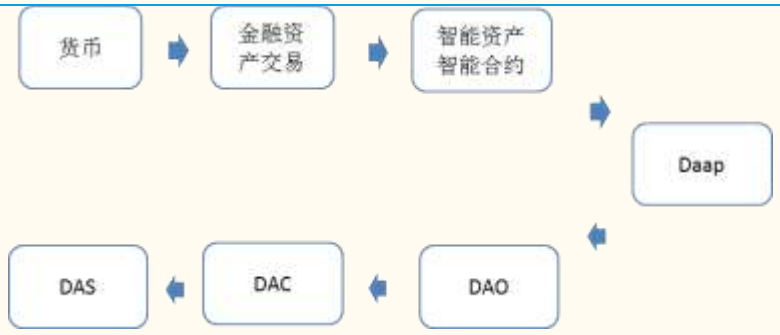
- **医疗领域。**有专家推测区块链在医疗领域也有市场将可能是除金融行业以外最大的行业，个人电子病历与基因数据都是极其隐私的数据，需要进行安全存储与访问控制，区块链的非对称加密技术能够保证个人医疗数据的安全性。
- 目前比较知名的案例是飞利浦医疗和 TIERION 进行合作，飞利浦医疗通过区块链技术来完成关于病历资料的认证， 或者是病历方面的隐私保护。

图表 32：区块链在 医疗行业应用

来源：互联网，国金证券研究所

- **DAO、DAC、DAS。**由于货币在经济中的核心与基础地位，所以我们看到区块链的应用首先在货比上，然后是对安全传输要求较高的金融资产交易，接着扩展到所有资产的注册于交易，随着智能合约变得复杂，区块链自治性提高，借助货币与智能合约以及安全存储能够实现社会组织的自治管理，Dapp（去中心化应用）、DAO（去中心化组织）、DAC（去中心化公司）、DAS（去中心化社会）将会逐渐出现。

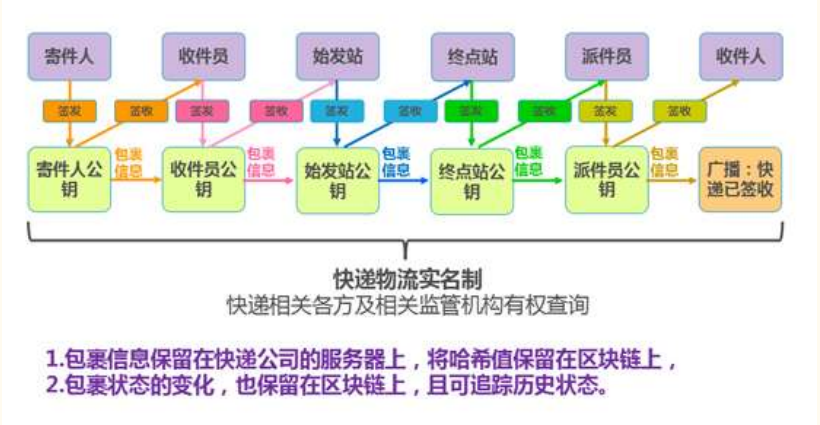
图表 33：区块链应用路径



来源：国金证券研究所

- **物流。**当前物流领域有快递丢包、误领、错领，以及快递员伪造签名逃避考核等问题，利用区块链技术，在快递交接时需要双方进行私钥签名，签名信息被记录在区块链上，物流中间流通信息不可篡改，同时可供查询解决了当前物流领域一系列问题。

图表 34：基于区块链物流应用架构



来源：复杂美区块链研究中心，国金证券研究所

- 区块链的普及进程方面，就像互联网发展初期一样也是依赖技术的发展与需求端的变化逐步应用到各个领域，所以区块链的应用也一定是以某些应用为突破口逐渐深入。比特币的底层区块链技术为价值互联网提出了一个很好的思路，但是现有区块链技术由于吞吐量、延时与容量等问题应用领域还比较窄，发展初期主要从一些低频次、数据量小、价值小以及无中心的的领域进行尝试，随着底层区块链技术的发展应用也将越来越广泛。
- 区块链解决了无中心的价值传输的问题，将会成为建立在信息互联网之上的价值互联网的的核心，将重塑金融乃至整个社会产业生产方式。在金融领域的应用的普及进程来看，我们认为区块链的应用将会率先在中介较多的无中心领域，中介使得交易成本提升，无中心让区块链的普及阻力大大降低，所以我们认为金融领域的应用将率先在股权交易、票据以及贷款等领域得到应用。货币与股票交易由于中心地位强势，又有法律保护，所以应用阻力较大。

4、区块链应用与相应初创公司介绍

- 区块链催生了信息互联网之上的价值互联网，颠覆现有价值交换的方式以及生产活动组织形式，从货币到金融资产的交易，再到各行业的应用。在智能合约、证券交易、电子商务、物联网等领域以及出现了大量的创业企业，相关的应用不断地成熟。

图表 35：区块链应用领域与相应公司

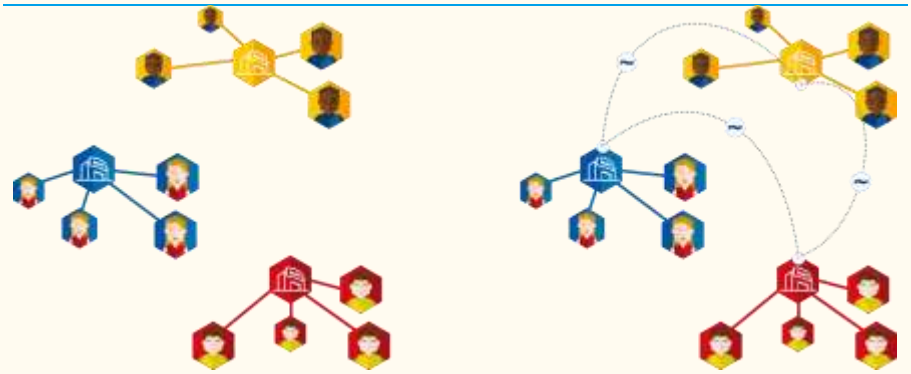
应用领域	公司
智能合约	闪电网络（Blockstream）、侧链(Blockstream)、以太坊（Ethereum）、Rootstock、Tendermint 、 BlockSign、Chronicled、SuperNET、Blocknet，Tezos；
证券交易	tØ.com(Overstock)、http://Chain.com、DAH（Digital Asset Holdings）、OpenLedger、 SETL、Symbiont、Maker/Dai ；
电子商务	OpenBazaar，Eris，BitXBay，Bitmarkets
物联网	ADEPT（IBM）、 Filament、Tilepay；
社交通讯	Gems、Codius、Bitmessage、Tweether、Twister；
文件存储	MaidSafe、Filecoin、Factom、Storj、Tau、Dfinity；
存在性证明	Monegraph、chronobit、Stampery；
众筹	小蚁(AntShares)、Swarm、Koinify、Lighthouse；
预测市场	Augur、Truthcoin、Futarchy；
身份验证	Blockscore，ShoCard，DIONS，LaunchKey；
数据 API	区块元(blockmeta)、BTC 区块（比特大陆）、区块（火币）、OKlink（OKcoin）、http://blockchain.info、Coinalytics、blocktrail、blockcypher、tradeblock、Scorechain

来源：国金证券研究所

4.1、锐波科技

- 锐波是一家从事分布式清算系统与价值网络研发与应用的互联网科技公司，它推出的 Ripple 价值传输协议是一种用以进行金融交易的互联网协议，该协议可以用来即时免费地以任何币种向世界的任何角落转账。
- 锐波与 Ripple 联合发布 ILP 协议，ILP 协议创建了一个这样的系统，在这个系统中，两个不同的记账系统可以通过第三方“连接器”或“验证”机器来互相自由地传输货币。记账系统无需去信任“连接器”，因为该协议采用密码算法为这两个记账系统和连接器创建资金托管，当所有参与方对资金量达成共识时，便可相互交易。
- 该系统使得不同货币之间、不同支付系统之间的结算的成本大幅下降，同时转账时间平均只需要 5 秒，相比比特币 10 分钟支付延时有大幅的提升。

图表 36：锐波科技清算原理图



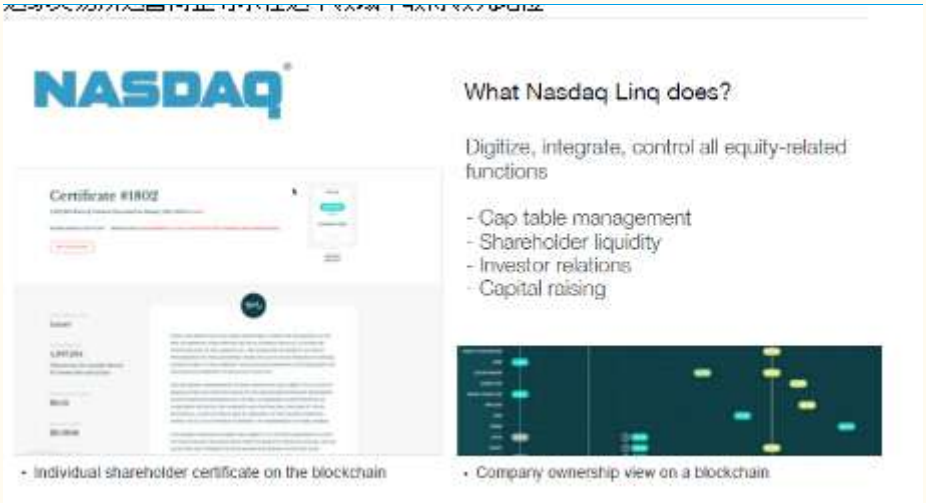
来源：锐波科技，国金证券研究所

- 首先中小支付机构在夸系统结算中产生很大的成本，成为了 Ripple 最早的支持者，随后规模较大的银行也逐渐加入。目前，全球数十家主流银行已经加入 Ripple 协议，包括德国（Fidor 银行）、美国（Wells Fargo, Bank of America，US Bank, PNC 银行）等银行，Ripple 目前支持全球至少 25 种货币之间的兑换，包括：USD、EUR、CNY、CAD、JPY 等主流货币。

4.2、纳斯达克 linq

- Linq 是纳斯达克正式推出其基于区块链技术的股权交易平台，通过网上交易，极大地缩短了结算时间，解决了场外股权交易的信任问题，并且交易双方在线完成发行和申购材料也能有效简化多余的文字工作。
- 基于区块链技术所提供的高效率，将能够大幅度提升 Linq 作为私人股权交易平台的优势。传统的手工处理方式往往会留下很大人工失误的空间。区块链技术有潜力能够消除这个痛点，因为其最大的“核心优势”就是能够提供一种不可篡改的记录，以及为用户提供一个永久保存的数据链。

图表 37：纳斯达克 linq

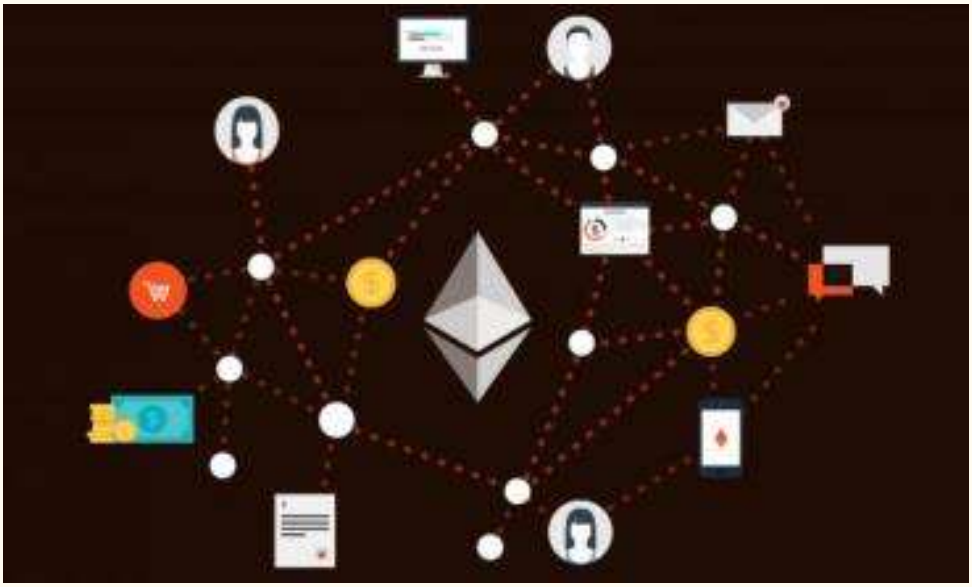


来源：公开资料，国金证券研究所

4.3、以太坊（Ethereum）

- Ethereum（以太坊）内置了编程语言的区块链平台，使开发人员能够建立和发布区块链应用。Ethereum 与其他平台不同，它不仅支持特定的区块链系统或者应用，能够基于内置的编程语言开发运行各种应用，如投票，域名，金融交易所，众筹，公司管理，合同和大部分的协议，知识产权，还有得益于硬件集成的智能资产。
- 从编程语言的角度来看，以太坊（Ethereum）是下一代密码学账本，打算支持众多的高级功能，包括用户发行货币，智能协议，去中心化的交易和去中心化自治组织(DAOs)或去中心化自治公司（DACs）应用。以太坊（Ethereum）提供内置的图灵完备（一切可计算的功能）的脚本语言的区块链计算平台，允许通过被称为“合同”的机制来为自己想实现的特性写代码，为可编程货币、可编程金融、可编程合约提供了底层的技术平台。

图表 38：以太坊（Ethereum）



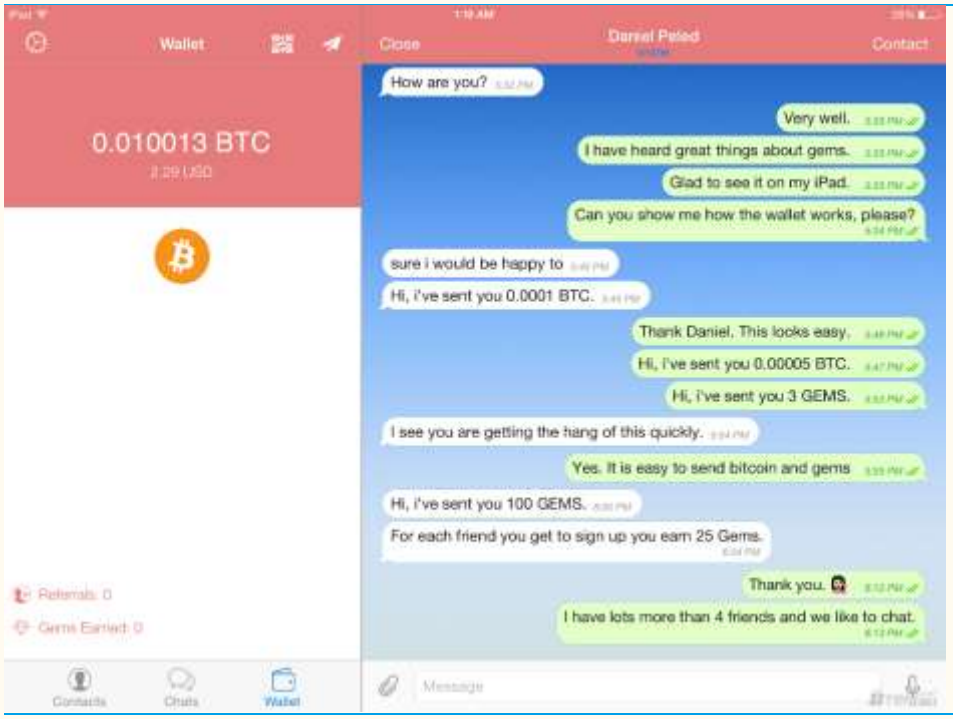
来源：公开资料，国金证券研究所

- 当前使用以太坊开发平台的机构除了众多创业团队，还有 R3 众多金融机构以及 IBM 与三星等大公司的加入，也催生了基于以太坊区块链的众多应用，收到众多机构的应用当前以太币市值已经排到所有电子货币中的第二位。

4.4、GetGems

- GetGems 是一个去中心化社交通信应用的初创项目，它基于比特币区块链技术开发社交工具，享受完全加密的私人信息及内置钱包的体验，中心化的社交软件安全性依赖于中心的安全措施，GetGems 提供完全加密的通信与存储，安全性大大提高。
- 另外，Gems 引进了一项创新的报酬机制，采取给用户提供奖励而不是收费的方式。任何使用 Gems 的用户都可以通过邀请好友、利用网络、建立网络生态系统等得到 Gems 币。Gems 币可以作为 app 内置货币，打个比方，广告主可以直接将 Gems 币付给用户。
- Gems 的理念在于能够让用户完全掌控自己的数据，在为广告主创造价值的同事应该有价值的回报，而不是原来的软件开发提供服务，获得广告收益的模式。

图表 39：GetGems 界面

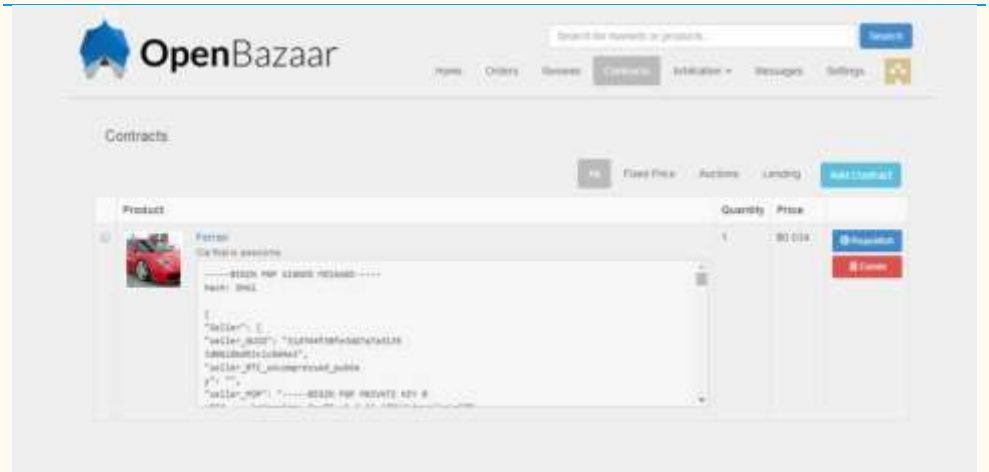


来源：互联网，国金证券研究所

4.5、OpenBazaar

- OpenBazaar（公开市场）是为网上点对点（P2P）交易平台，好比 eBay 和 BitTorrent 结合的产物。
- 当买卖双发同意交易后，OpenBazaar 就会使用买卖双方的数字签名创建一个合约，并将该合约发送到被称为公证人的第三方，公证人可能系统用户任何人。第三方为合约作证，并创建多重签名比特币账户，只有当集齐三个签名中的两个时，比特币才会被发送给卖家。
- OpenBazaar 有一个信誉评分系统，允许所有的用户对其它用户进行反馈评分，买卖家与第三方评论者都会被评价，并且评价是不可更改的。如果某些人打算诈骗其他的用户，他们的信誉将会受损，第三方如果不能公正裁定交易纠纷，他们的信誉也会受损。。

图表 40：OpenBazaar 界面



来源：互联网，国金证券研究所

- 该平台相比现有电子商务平台，去除现有中心平台，使得原本平台的数据精准投放的收益归还给用户，保护了用户数据，把权力归还到用户手中，进而搭建了一个自组织的商品交易平台。

4.6、小蚁(AntShares)

- 小蚁是一种区块链协议，用户可以将实体世界的资产和权益进行数字化，通过点对点网络进行登记发行、转让交易、清算交割等金融业务的去中心化。小蚁目标市场不仅是数字货币圈，还包括股权众筹、P2P 网贷、资产管理以及智能合约等。
- 通过在区块链上注册股权以后，初创公司能够用小蚁来管理股东权益，可以在平台上通过众筹、转让等方式完成股权融资，投资者也可以进行点对点的股权交易。 P2P 网贷方面：类似股权交易，同样支持债权的注册、转让以及交易，企业还可以用自己的小蚂蚁发行公司债券。

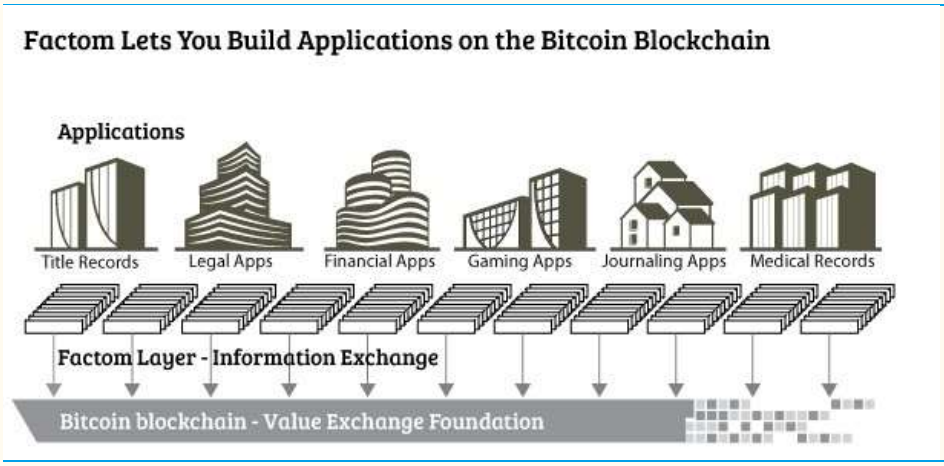
图表 41：小蚁(AntShares)

来源：互联网，国金证券研究所

4.7、Factom

- 全球经济中信任稀缺，这造成大量资源的投入到审计、记录、证明中，降低了生产下来。同时不管是纸质还是电子版材料保证真实性都非常困难，Factom 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。大大减少了进行独立审计、管理真实记录、遵守政府监管条例的成本和难度。
- Factom 正在革新整个世界对数据的记录方式，利用比特币区块链技术来保护您的数据安全，同时不用受到直接把数据写入比特币区块链的各种限制：例如写入的数据速度，成本，大小等限制。

图表 42：Factom 系统架构



来源：公证通 Factom 白皮书，国金证券研究所

4.8、其他应用

- 此外还有用于预测市场、P2P 贷款、随机公正、政务管理、证书验证以及智能资产等应用。

图表 43：区块链其他领域应用

来源：互联网，国金证券研究所

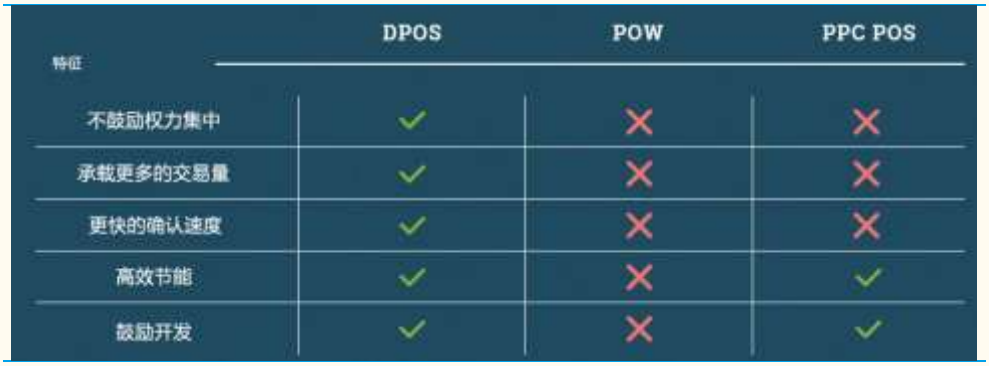
5、技术突破超预期，巨头大幅投入，新贵不断崛起

5.1、技术不断获得突破

- **POW 、POS、DPOS。**共识机制是区块链中用来确认信息产生区块的机制，当前主要主 POW 、POS、DPOS 等机制。**POW** 也称工作证明，简单来说，就是你的收益取决于你对区块链作出的贡献，通常是指挖矿贡献的有效工作，一般在 POW 机制下收益与算力在全网算力占比成正比，该机制应用较广泛如如比特币、莱特币。**POS** 也称股权证明，类似于财产储存在银行，这种模式会根据你持有数字货币的量和时间，分配给你相应的利息。**DPOS** 机制通过无摩擦的实时投票产生一组总数一定的“授信方”，受信方来进行区块的验证与打包确认。

  POW 机制下收益与算力在全网算力占比成正比，使得节点计算能力趋于集中，这使得 51%攻击可能大大提高威胁系统安全性，同时全网计算使得资源浪费较严重。POS 机制下集中货币市值进行网络攻击，要比获得算力困难的多，同时货币持有者不会攻击系统以损害自生利益，提升参与计算节点可信度，另一方面减少参与计算节点提升系统处理效率。**DPOS 通过投票选出**“授信方”进行区块确认，提升了交易吞吐量降低交易成本，由于“授信方”维护自身利益来保证系统的安全性。

图表 44：各种共享机制优缺点



来源：互联网，国金证券研究所

- **公有链 、私有连、联盟链。公有链：**是指全世界任何人都可读取的、任何人都能发送交易且交易能获得有效确认的、任何人都能参与其中共识过程的区块链——共识过程决定哪个区块可被添加到区块链中和明确当前状态。**联盟链：**指其共识过程受到预选节点控制的区块链。**私有链：**是指其写入权限仅在一个组织手里的区块链。读取权限或者对外开放，或者被任意程度地进行了限制。

图表 45：公有链 、私有连、联盟链优缺点介绍

	公有链	联盟链	私有链
优点	保护用户，免受开发者的影响	实现51%攻击较困难	规则可控
	网络效应	交易成本更便宜、吞吐量	验证者是公开的，不存在51%攻击
		节点可以很好地连接	交易成本更便宜、吞吐量更大
		节省计算资源	节点可以很好地连接
			节省计算资源
缺点	确认时间长	节点易受攻击	节点易受攻击
	交易费用高		
	计算资源浪费		

来源：国金证券研究所

出于计算节点的信任问题以及吞吐量与延时等问题考虑相继出现了联盟链与私有链。联盟链中计算与控制节点有一定的准入门槛，保证计算节点可靠性，降低了资源的消耗与效率的牺牲，比较适合银行这种有一定集中度

的市场。私有链完全有某个组织控制计算节点，能够对规则进行控制与修改，比较适合政府与一些有强中心的市场。公有链由于当前效率低等问题，主要应用于交易频率低、数据量小等应用中，随着技术的发展应用逐渐防范，同时我们认为公有链与私有链的界限真正模糊，从公示机制的发展也可以看出 POS 与 DPOS 与混合链的思路想通，所以随着技术的发展技术逐渐融合。

- **价值互联网行业的发展依赖于区块链性能的提升。**互联网的发展主要分为网络传输技术与终端技术的发展与普及，随着技术的发展与网络的普及应用逐渐丰富。对比互联网行业的发展，当前区块链还处于早期，由于智能终端与底层传输技术已经成熟，未来价值互联网的发展主要依赖区块链技术的吞吐量、安全性、存储空间需求等性能的提升与优化，随着技术的进步建立在价值互联网上的应用于价值也将呈现爆发式增长。

- **区块链技术的发展与性能的提升大超预期。制约当前已区块链为核心的价值互联网应用发展的阻碍主要有：**吞吐量、确认延时、安全性、存储空间需求等问题，从区块链与 IBM OBC 的技术指标来看性能已经得到大幅提升，一方面通过私有链与联盟链提升吞吐量减少延时提升安全性，另一方面通过 POS、DPOS 等共识机制提升系统效率，降低计算资源占用。从以太坊的底层平台推出时间表来看，通过分片与状态通道以及新的共识机制系统性能还能够得到大幅提升，达到“没有限制”的扩展性。

图表 46：区块链平台参数对比

	比特币	以太坊	OBC
共识算法	POW	POW	PBFT
交易延时	10分钟	15秒	20毫秒
吞吐量	3-7		上千
节点存储空间需求	30G	3G	
架构设计	电子加密货币 智能合约若支持公有链	电子加密货币 智能合约 公有链	智能合约 可构建电子货币 联盟链
账本扩展性	差 需要全账本	好 不完全需要全账本	

来源：公开资料 国金证券研究所

图表 47：以太坊平台推出时间表

以太坊平台推出时间表
Metropolis:Mist **浏览器**的发布，预计在 2016 年的夏天或秋天
Serenity（“以太坊 1.5”）:发布区块链的 **PoS 股权证明**(Casper)版本，同时包含以太坊改善提议（**EIPs**）10 和 105。这计划在 2017 年早期实现。
WebAssembly 发布（“以太坊 1.75”）:**更快的虚拟机**。预计在 2017 年
以太坊 2.0（尚未命名）：**初步可扩展性**提升的版本。预期在 2017 年晚期实现。
以太坊 3.0（尚未命名）：**“没有限制的”**可扩展性版本，预计在 2018 年晚期实现。通过：sharding（分片）和state channels（状态通道） 技术将协议改造成一个可运行VISA 支付网络级别的区块链，甚至是其几个级别之上的性能

来源：以太坊，国金证券研究所

5.2、各国政府积极表态，抢占价值互联网技术制高点

- 虽然各国对比特币持否定跟观望的态度，但对于其底层的区块链技术的研究均比较积极。 2016 年 2 月 13 日中国央行行长表示：区块链技术是一项可选的技术，人民银行部署了重要力量研究探讨区块链应用技术，美国证券交易委员会已经证实了 Overstock 计划用区块链技术发行股票，英国政府发布区块链技术报告，除了创建基于区块链公共平台为社会服务，还计划构建在政府和公共机构之间使用的应用系统。

图表 48：各国政府对区块链态度

国家	政府对区块链态度
中国	周小川：区块链技术是一项可选的，人民民银行部署了要力量研究探讨区块链应用技术
美国	美国证券交易委员会已经证实了 Overstock 计划用区块链技术发行股票
英国	2016 年 1 月 19 日，英国政府发布了一份 名为 《分布式账本技术：超越区块链》区块链技术的重要报告。除了创建一个基于区块链的公共平台，来为全民和社会提供服务时。英国政府还计划开 发一个能够在政府和公共机构之间使用的应系统。

俄罗斯	2016 年 5 月，俄罗斯联邦金融监督服务中心副主任利瓦德尼宣布正计划创建 自己的加密货币
澳大利亚	澳大利亚证券交易所以 1950 万美元收购了区块链创业公司，数字资产公司 5%的股权。
韩国	韩国唯一证券交易所 2 月宣布，在用区块链技术开发场外交易平台。

来源：国金证券研究所

5.3、巨头与新贵共舞

- R3 公司是一家去年下半年成立于纽约的金融技术创业公司，专注于研究基于区块链的金融技术解决方案。目前已经建立了一个由 40 多家国际银行机构组成的团体，目的是为了建立一种定制的基于以太坊的跨境区块链解决方案。
- 目前，R3 联盟的成员已经包括的金融机构有：花旗银行，美国银行，高盛集团，摩根大通，瑞银集团，摩根史坦利等金融机构。接下来，R3 联盟计划探索其他领域，包括分布式账本互操作性、隐私性、身份验证、扩展性。其中包括与微软合作利用其 Azure 区块链即服务在银行合作机构之间实施区块链技术。这一切都代表着一个巨大金融变革的开始。

图表 49：R3 成员

来源：互联网，国金证券研究所

中国平安金融集团已加入金融创新公司 R3，成为国内该联盟的第一个合作伙伴。随后香港友邦也加入 R3，国内金融科技公司纷纷涉足区块链研发。

图表 50：中国分布式总账基础协议联盟成员

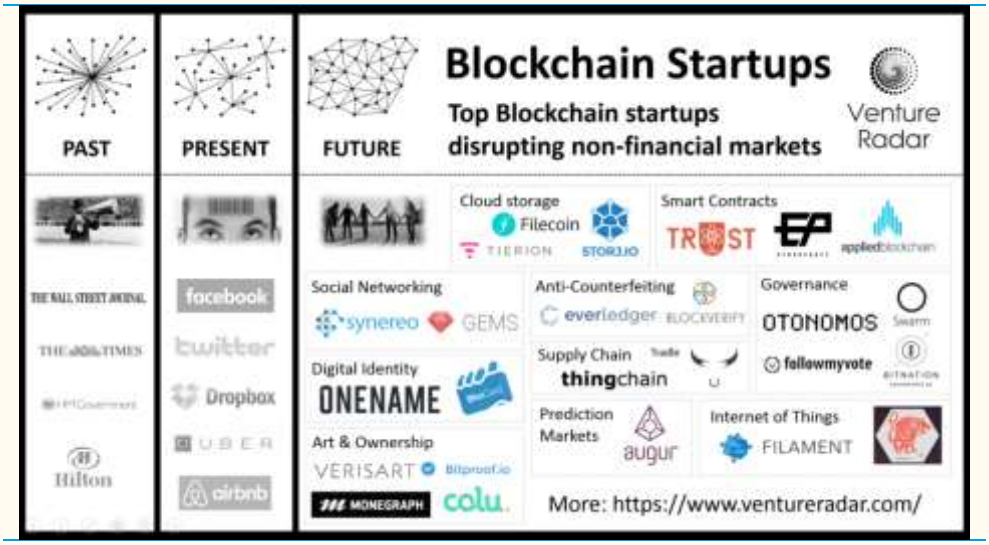
来源：互联网，国金证券研究所

- 13 年以来，区块链领域的而投资额爆发式增长，15 年已接近 4 亿美金，资本的不断进入显示了资本对于区块链技术的认可，人才与资本不断进入推动技术进步，应用不断丰富，推动区块链应用普及。

图表 51：区块链领域投资规模

来源：互联网，国金证券研究所

图表 52：区块链领域创业公司



来源：互联网，国金证券研究所

6、标的推荐

赢时胜

- 公司为金融机构的资产管理和资产托管业务整体信息化建设提供应用软件及增值服务，产品服务需求主要来源于金融产品增加、金融政策制度变化、金融机构增加、信息技术应用发展变化以及客户业务和服务模式变化。公司客户资源广发，涵盖银行、基金公司、证券公司、保险公司、信托公司、期货公司、财务公司等 300 余家金融机构客户，其中，托管银行 24 家，占托管银行总数的 88.88%，其他银行客户 17 家，基金公司 95 家，占基金公司总数的 95.00%、证券公司 62 家，占证券公司（只开展经纪业务的证券公司除外）总数的 50.00%、信托公司 17 家，占信托公司总数的 31.48%、保险公司 52 家，占保险公司总数的 36.61%。
- **切入 PB 业务市场，构建“金融服务云平台”。**私募业务外包服务快速发展，截止 2015 年底备案私募基金机构达到 2 万家，资产管理规模突破 4 万亿元，PB 业务市场潜力巨大。公司已于 2015 年取得基金行业协会服务外包备案资格， 由公司与深圳证券通讯有限公司联手构建的云平台已于 2015 年年初成功上线并服务于全国证券公司、私募投资等金融机构，截至目前资管云已有 7 家客户正式运作。
- **转型互联网服务提供商。**利用在金融领域广泛的客户群体构建从金融 IT 服务往拓展金融服务方向转型，公司投资 1800 万元占股 60%，于上海自贸区成立控股公司上海赢量金融服务公司，开展互联网票据平台业务。2015 年 6 月和 9 月，公司各投资 2000 万元参股东吴在线和阳光金服，将业务范围逐步延伸至互联网金融服务领域。
- 预计公司 2016-2018 年 EPS 分别为 0.37 元、0.58 元和 0.86 元，考虑到互联网金融业务的逐渐落地将为公司带来巨大的业绩增长空间，对应 129 倍、82 倍、56 倍的估值，给予“买入”评级。

恒生电子

- 公司主要为金融机构提供 IT 软件产品与服务。公司的客户群体主要包括券商、公募基金、银行、期货公司、信托公司、保险公司、私募基金等，并逐步拓展到和金融生态圈有关的互联网企业，公司的投资赢家产品线（证券交易客户端）以及参股的网金社等业务也覆盖到了 C 端的个人客户。公司为金融机构提供的业务量占到公司总业务量的 80%左右。
- 参与设立粤财保险，深耕金融产业链。恒生电子是目前中国拥有“全牌照”的金融 IT 企业，业务范围涵盖银行、证券、基金、信托、保险、期货等金融市场的各个领域，在金融混业趋势和金融创新发展的格局下，参与设立粤财保险，运用“互联网+”技术推动信用保证保险业务支持中小微企业和“三农”企业发展，更有利于恒生发挥协同优势，构建业务壁垒。
- 预计公司 2016-2018 年 EPS 分别为 0.93 元、1.25 元和 1.69 元，参考同行业可比公司，考虑恒生在金融 IT 领域的创新优势和龙头地位，对应 70 倍、52 倍、39 倍的估值，给予“买入”评级。

海立美达

- **收购联动优势，打造“制造+金融科技”双轮驱动。**公司传统汽车配件业务收入实现 20%以上的增长，同时高毛利业务收入 整体毛利占比提升。公司于 2 月 28 日公告以 30.3 亿收购联动优势 91.56%股权，联动优势是国内领先的移动信息服务、移动运营商计费结算服务和第三方支付服务提供商，其在金融行业移动信息服务领域占据绝对优势，去年发送 977 亿条短信，今年继续保持 30%增长，公司第三方移动支付市场份额第五，15 年交易额达 3800 亿，重组后有望借助上市平台做大做强。
- **立足支付，发力科技金融创新。**公司未来发展战略是做大第三方支付，立足支付发力大数据与区块链的金融科技创新业务。公司在金融行业耕耘多年，掌握了大量的支付数据，为未来大数据表现提供支撑，同时公司研究区块链技术以及新的应用领域，拓展价值互联网蓝海市场。

- 预计公司 2016-2018 年 EPS 分别为 0.78、1.17 及 1.53 元，考虑到，金融科技创新加速可能为公司带来巨大的业绩增长空间，对应 40、30 及 28 倍的估值，给予“买入”评级。

四方精创

- 国内领先的银行 IT 服务商。公司是国内领先的银行 IT 服务商，主业包括括软件开发服务、应用维护及系统集成。公司长期服务港澳台地区银行，引进国际先进的银行业务流程理念，重点服务国内大中型银行，是中国银行、中银香港、农业银行、永亨银行、东亚银行、大新银行、等银行的核心供应商。
- 积极研究区块链技术，引领科技金融创新。5 月 31 日下午，聚焦于区块链在金融方面应用的金融区块链合作联盟（深圳）正式成立，其中发起单位 25 家，腾讯、华为等 6 家机构作为成员单位加入。联盟拟定了区块链 12 项研究课题，其中四方精创参与区块链底层技术平台、区块链云服务、区块链理财产品一二级市场、区块链在积分领域的应用等课题研究，参与“金链盟”课题研究有望整合各方资源，提升区块链技术研发实力，开拓新兴应用领域。
- 预计公司 2016-2018 年 EPS 分别为 0.42 元、0.64 元和 0.83 元，给予“增持”评级。

飞天诚信

- 受需求萎缩，公司传统 USB Key、OTP 动态令牌等主营产品 15 年出现出现下滑，16 一季度业绩来看下滑颓势基本稳定。面度传统产品需求饱和的压力，公司研发以嵌入式操作系统为核心的智能卡，已获得“银联、万事达以及 VISA”的供应商资格，同时公司飞天迪士尼主题公交卡将在 30 多个城市发行，并与中银通签署了战略合作协议，为公司智能卡业务打下市场基础。
- 依托密码技术，布局区块链。公司主业是以安全为核心的银行身份认证设备，持续在区块链研发领域投入，当前已有一定的技术储备，未来主要应用首先从公司现有支付认证业务出发，解决银行系统数字货币支付认证安全性问题，其次探索区块链在其他金融领域的应用。
- 预计公司 2016-2018 年 EPS 分别为 1.02 元、0.94 元、0.98 元，分别对应 PE35、38、36 倍，给予“增持”评级。

御银股份

- 公司提供给银行类金融机构用于为其客户提供自助式金融服务，主要由 ATM 产品销售和 ATM 运营服务两部分组成，涵盖 ATM、CRS 等金融类产品以及 VTM（远程可视柜员机）、清分机等泛金融类产品的多元化产品系列，自主研发能力和研发设施达到或部分达到国际先进水平。
- 增资御银信息，发展互联网金融。对全资子公司广州御银信息科技有限公司增资 7,000 万元人民币，加大对互联网金融企业的投资、兼并，适时参与互联网金融产业基金的发起设立。推进广州御银科技股份有限公司互联网金融业务发展，充分利用公司多年在银行的优势，整合现有资源，调整产业链结构，培养互联网金融成为公司新的利润增长点。
- 预计公司 2016-2018 年 EPS 分别为 0.22 元、0.27 元、0.33 元，分别对应 PE57、41、37 倍，给予“增持”评级。

长亮科技

- 公司主要为商业银行以及其他泛金融机构提供提供定制化的软件产品、整体解决方案以及人力资源外包服务。由于公司成功研发新一代的商业银行核心业务系统、成功推广泛金融机构业务系统信息化解决方案，成立了多家专注单一具体金融信息化业务领域的全资或者参股子公司，使得 2015 年公司营收实现了 75.04%的增长。

- 拓展泛金融信息化领域，推进国际化战略。公司成功完成了发行股份购买长亮合度 100%股权的相关工作，并且通过内部资源整合与人才引进战略，投资成立了前海长亮、成都长亮、上海长亮等多家具有自身特色的子公司，进一步加强了公司在金融行业资产管理、互联网金融、商业智能、信用卡等方面的布局，提升了相关领域的竞争能力，开拓了泛金融行业领域的市场和销售模式，客户扩展至互联网金融公司、小贷公司、财务公司、汽车制造商、资产管理公司等群体。公司在香港投资设立了境外机构，迈出了国际化战略的第一步。并且，在 2016 年，公司将持续通过并购与人才吸引战略，组成海外研发与技术团体，把公司在国内的领先产品推广国外客户中去。
- 预计公司 2016-2018 年 EPS 分别为 0.43 元、0.56 元、0.74 元，分别对应 PE118、83、65 倍 PE，给予“增持”评级。

广电运通

- 公司定位“高端制造+高端服务”双轮驱动，产品及服务覆盖金融电子、轨道交通两大领域，是一家以银行自动柜员机（ATM）、远程智慧银行（VTM）、清分机、智能交通自动售检票系统（AFC）等自助设备产业为核心，融合自助设备维保服务、金融外包服务、金融武装押运业务三大服务业，集自主研发、生产、销售及服务为一体的现代化高科技企业。
- 深化服务领域布局。公司形成了以广州银通作为金融服务业主体、以深圳银通为传统维保业务平台、以广州安保投资公司为金融外包业务主要平台的，且与发展战略吻合的服务业架构。公司维保业务在原有统筹、集约管理的基础上，推进服务精细化管理，建立分公司系统稽查平台。在金融外包服务市场上，随着互联网金融冲击及金融改革的不断深化，银行业面临网点转型与削减成本的压力，公司拥有开展金融外包服务的子公司 12 家，金融外包业务共覆盖 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
- 预计公司 2016-2018 年 EPS 分别为 0.68 元、0.80 元、0.95 元，分别对应 PE25、21、18 倍 PE，给予“增持”评级。

金证股份

- 成熟的证券 IT 服务商。交易系统和覆盖券商以客户为中心的账户、资金、登记托管系统，均在各家新老客户上线实施。积极响应交易所、登记公司等上游机构发展标准化金融产品的业务，同时也为券商自身业务差异化提供 IT 技术平台，公司在面向用户服务的前、中、后台布局下，用户前端系统，基础技术平台，业务服务中台，业务交易后台和基础业务平台等各条产品线均有重大突破，以传统 1.0 软件+服务的方式收取费用盈利。
- 拓展综合金融 IT 业务。保持在产股权交易等领域的市场龙头地位，同时面向综合金融全行业快速业务拓展，尤其是在金融资产交易和互联网金融创新业务方面斩获一系列新单，保障了第一代“软件+服务”盈利模式的稳健增长，“合作共建、流量分成；系统租赁，按需付费”的综合金融第二代盈利模式已成功落地。
- 预计公司 2016-2018 年 EPS 分别为 0.48 元、0.70 元、1.00 元，分别对应 PE79、57、42 倍 PE，给予“增持”评级。

长期竞争力评级的说明：

长期竞争力评级着重于企业基本面，评判未来两年后公司综合竞争力与所属行业上市公司均值比较结果。

公司投资评级的说明：

买入：预期未来 6—12 个月内上涨幅度在 15%以上；
增持：预期未来 6—12 个月内上涨幅度在 5%—15%；
中性：预期未来 6—12 个月内变动幅度在 -5%—5%；
减持：预期未来 6—12 个月内下跌幅度在 5%以上。

行业投资评级的说明：

买入：预期未来 3—6 个月内该行业上涨幅度超过大盘在 15%以上；
增持：预期未来 3—6 个月内该行业上涨幅度超过大盘在 5%—15%；
中性：预期未来 3—6 个月内该行业变动幅度相对大盘在 -5%—5%；
减持：预期未来 3—6 个月内该行业下跌幅度超过大盘在 5%以上。

特别声明：

国金证券股份有限公司经中国证券监督管理委员会批准，已具备证券投资咨询业务资格。

本报告的产生基于国金证券及其研究人员认为可信的公开资料或实地调研资料，但国金证券及其研究人员对这些信息的准确性和完整性不作任何保证，对由于该等问题产生的一切责任，国金证券不作出任何担保。且本报告中的资料、意见、预测均反映报告初次公开发布时的判断，在不作事先通知的情况下，可能会随时调整。

客户应当考虑到国金证券存在可能影响本报告客观性的利益冲突，而不应视本报告为作出投资决策的唯一因素。本报告亦非作为或被视为出售或购买证券或其他投资标的邀请。

证券研究报告是用于服务机构投资者和投资顾问的专业产品，使用时必须经专业人士进行解读。国金证券建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。报告本身、报告中的信息或所表达意见也不构成投资、法律、会计或税务的最终操作建议，国金证券不就报告中的内容对最终操作建议做出任何担保。

在法律允许的情况下，国金证券的关联机构可能会持有报告中涉及的公司所发行的证券并进行交易，并可能为这些公司正在提供或争取提供多种金融服务。

本报告反映编写分析员的不同设想、见解及分析方法，故本报告所载观点可能与其他类似研究报告的观点及市场实际情况不一致，且收件人亦不会因为收到本报告而成为国金证券的客户。

本报告仅供国金证券股份有限公司的机构客户使用；非国金证券客户擅自使用国金证券研究报告进行投资，遭受任何损失，国金证券不承担相关法律责任。

上海

电话：021-60753903

传真：021-61038200

邮箱：researchsh@gjzq.com.cn

邮编：201204

地址：上海浦东新区芳甸路 1088 号紫竹国际大厦 7 楼

北京

电话：010-66216979

传真：010-66216793

邮箱：researchbj@gjzq.com.cn

邮编：100053

地址：中国北京西城区长椿街 3 号 4 层

深圳

电话：0755-83831378

传真：0755-83830558

邮箱：researchsz@gjzq.com.cn

邮编：518000

地址：中国深圳福田区深南大道 4001 号时代金融中心 7BD