CMS 招商证券

推荐（首次）

让全世界做你的证人

2016 年 04 月 10 日

IT宿命系列报告之——区块链深度专题

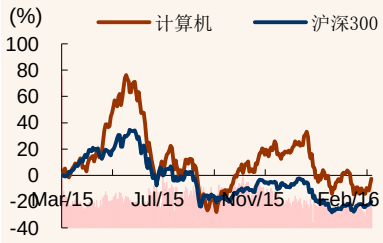
上证指数	2985

行业规模

		占比%
股票家数（只）	137	4.9
总市值（亿元）	19616	4.5
流通市值（亿元）	12378	3.6

行业指数

%	1m	6m	12m
绝对表现	-4.6	19.9	10.3
相对表现	-8.5	22.4	27.8



资料来源：贝格数据、招商证券

相关报告

1、《银行卡线下收单费率调整事件点评—银行卡支付场景加速渗透，收单衍生增值业务迎来发展新机遇》2016-03-20

2、《IT 宿命系列报告之：云计算专题（一）—化云为雨，政务领域打响云计算落地第一枪》2016-03-07

3、《计算机行业周报 2016 年 02 月 14 日—凛冬将至？钱会向值得投资的标的聚集》2016-02-25

刘泽晶
liuzejing@cmschina.com.cn
S1090516040001

研究助理
黄斐玉
huangfeiyu@cmschina.com.cn

研究助理
徐文杰
010-57601853
xuwenjie@cmschina.com.cn

我们用最生动的案例解读区块链为何物，认为区块链结合应用场景有望改变现有集中化 IT 网络数据管理模式，创造巨大经济效益，大胆猜想我国央行数字货币采用区块链可能的模式。国外巨头已快速布局，国内市场正处于爆发前夜。

- **区块链：不完美的完美机制。**比特币这一号称最完美的数字货币正是区块链最成功的应用之一，也是比特币“不可伪造，不可盗取”特性背后的功臣。区块链学术上讲是一种公共记账机制（技术方案），它将数据分布式存储，由全网共同进行维护和管理，实现自治，具有去中心化、去信任化、可扩展、匿名化、安全可靠等特点。但它同时也并不完美，在区块链大规模推广和应用之前，尚存有 51%攻击、工作效率、资源消耗、区块间博弈和冲突等缺陷。
- **脑洞大开，应用、场景为王：**我们认为区块链的去中心化可能颠覆现有互联网模式，结合应用场景有望产生巨大经济效益。谈及未来，区块链可以为很多领域添砖加瓦，如：数字货币、支付清算、数字票据、权益证明、征信、政务服务、医疗等。我们大胆猜测，区块链可能对各行各业都有一个升级改造，同时具备实现去中心化自治社会这一终极效果的可能。
- **关注央行数字货币，或许春天已不远：**央行行长周小川曾表示央行数字货币可能将采用区块链模式，彻底改变传统货币流通模式。央行数字货币的最终呈现形式目前虽尚无定数，但我们猜想有两种较大可能：1）摒弃传统的“中央银行—商业银行机构”的二元体系，商业银行机构的角色不再存在。2）央行与商行形成区块链 1，商业银行与社会个体形成区块链 2，通过两个区块链的相连提升灵活性，在必要的时候央行可以启动连接并将监管和调控的手直接作用于社会个体。央行通过发行数字货币，将降低传统纸币发行、流通、损毁等成本，减少违法犯罪行为，并能更好地调控货币的供应与流动性。
- **国际关注度极高：**目前国际上许多大商行已对区块链开展一系列探索，包括成立内部区块链实验室，投资金融科技初创公司，或者与初创公司进行合作。我们例举了几个代表性案例：1）摩根大通、高盛等 42 家国际顶级银行组成了国际最大的区块链联盟 R3，致力于打造一个开源、通用共享账簿的区块链联盟；2）支付网络 Ripple 可以有效地削减跨境货币支付成本，未来可能威胁到 SWIFT 的地位；3）纳斯达克在 2015 年 10 月正式推出区块链平台 Nasdaq Linq，通过 Nasdaq Linq 发股的发行者将享有“数字化”所有权。4）超级账本项目 Hyperledger 由 Linux 基金会联合全球超过 40 家金融、科技及区块链技术团队，致力于加速推动分散式分类帐技术的开源区块链专案。
- **建议关注具备区块链技术和应用的 IT 厂商。**我们认为区块链更像是一种机制或技术方案，未来能把这种机制结合到不同场景推广应用的厂商有望获得颠覆式的成功，建议关注：1）金融 IT 相关标的：**恒生电子、赢时胜、海立美达、信雅达、金证股份、广电运通**；2）加解密相关标的：**卫士通、飞天诚信**。

正文目录

图表目录

一、一种公共记账机制——区块链技术

近期“北京颐和酒店拖拽女子”一案引起社会的关注，而案件中的男子之所以敢明目张胆拖走女受害者，且旁人却冷眼旁观的主要原因在于：路过的人并不知道他们是不是夫妻。

区块链可以解决这个问题。

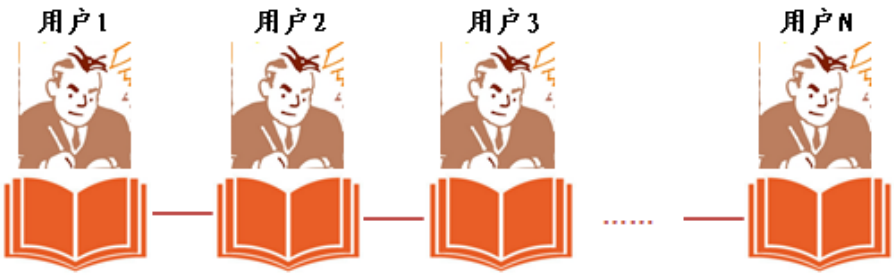
它能让全世界都知道你拥有什么财产、和谁发生过什么交易、甚至你和谁结了婚。你不用再跑去银行证明你的资产和办理汇款，也不用跑去派出所证明你是否结婚，在你需要的时候，打开你的电脑，全世界都会成为你的证人！

未来区块链的应用将具有无穷的想象空间，如数字货币、支付清算、数字票据、权益证明、征信、政务服务、医疗等等。

1、区块链是什么

区块链（Blockchain）的概念于 2008 年在中本聪的论文《比特币：一种点对点的电子现金系统（Bitcoin: A Peer-to-Peer Electronic Cash System）》中首次提出。区块链可以理解为一种公共记账的机制（技术方案），它并不是一款具体的产品。**其基本思想是**：通过建立一组互联网上的公共账本，由网络中所有的用户共同在账本上记账与核账，来保证信息的**真实性**和**不可篡改性**。而之所以名字叫做“区块”链，顾名思义，是因为区块链存储数据的结构是由网络上一个个“存储区块”组成一根链条，每个区块中包含了一定时间内网络中全部的信息交流数据。随着时间推移，这条链会不断增长。

图 1：由网络中的用户共同维护公共账本



资料来源：招商证券

2、区块链的原理与价值——以比特币为例

说起区块链，就不得不谈比特币。比特币与区块链是绑定在一起同时诞生的，也是目前区块链最成功的应用之一。

2.1、比特币的基本工作原理

比特币采用的去中心化存储便是区块链的核心思想：举个例子说明，传统货币的交易模式中，银行管理账户采用的是中心化管理。由银行建立中心数据库，每个人的银行账户信息和以及账户里有多少余额都由银行进行集中管理。当 A 要对 B 发起交易时：

1) A 向银行提出申请;

2) 银行查阅中心数据库验证 A 的身份、读取 A 的银行账户余额等信息进行核验;

3) 银行修改 A 和 B 的账户余额。

图 2: 传统方法中基于银行中心化的交易流程:

资料来源：招商证券

而基于区块链技术的比特币交易模式则剔除了银行作为中心数据库的角色，每个比特币用户的电脑都是一个节点，每个节点都能存储数据，节点和节点之间相连形成了巨大的网络。每个人的交易信息都对所有人公开，每当 A 发生一笔交易，网络内的所有人都能看到并予以记录，只有当网络内一定数量的人对这笔交易认可时，交易才算合法。还拿上面的例子说明，当 A 申请向 B 发起交易时:

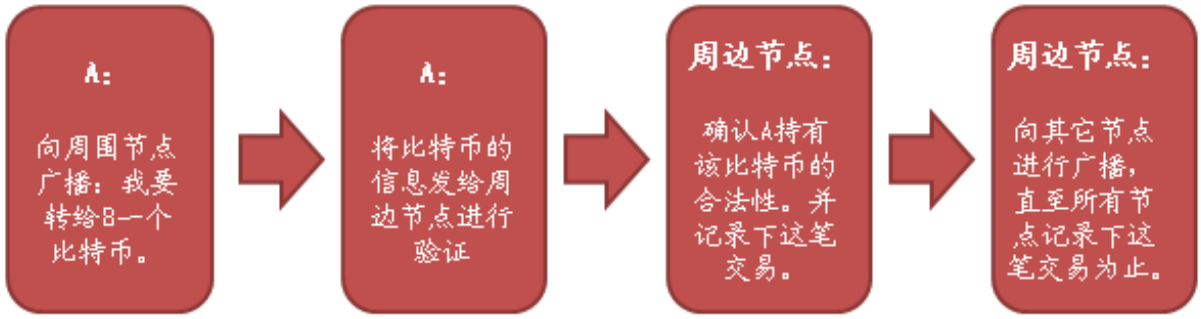
1) A 向周边节点广播：我要转账给 B 一个比特币。

2) A 将比特币的信息发给周边节点进行验证。

3) 周边节点确认 A 持有该比特币的合法性。当一定数量的节点验证通过后，交易成立，周边节点记录下这笔交易并确认比特币的新主人是 B。

4) 周边的节点再向网络中其它节点进行广播，直至所有节点记录下这笔交易为止。

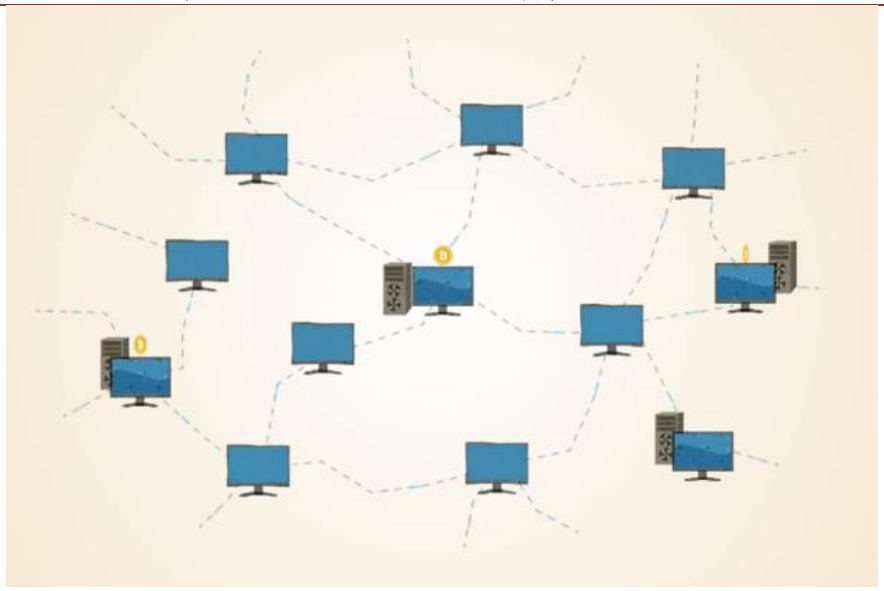
图 3: 基于区块链的比特币交易流程



资料来源：招商证券

通过区块链技术提升了数据的真实性与不可篡改性: 由于数据是分布式保存在每个人的电脑里，网络中的某个节点若收到攻击或出现意外而遗失了数据根本不会造成多大的影响。同样地，当发生一笔交易时，全世界的用户都可以担当监管者的角色，如果大家不认可交易的合法性，则交易无法达成，区块链上的数据由大家集体去维护。

图 4：区块链技术提升了数据的防遗失性以及防作弊性



资料来源：《比特币基础科普与常见误解》、招商证券

2.2、比特币的前世今生

比特币从何而来？摘录网络上的一段关于比特币的故事：

“2008 年一个神秘人物写了一套程序。于是 2009 年比特币诞生了。当然这套程序目前来说没有任何稀奇的。可以完整的复制出来。故事慢慢开始了。

假设发明之初，只有几个人无聊的在挖比特币。比如其中两个程序员，姑且称他们为甲、乙。于是他们建立了一个网上交易平台想卖出。他们没事在这里挖呀挖，挖了几千个，但是一直没人要买。甲说好无聊。乙也说好无聊。看故事的你们说：好无聊。谁会买几个虚拟数字呀。为了让大家不无聊，甲对乙说：要不我们玩个游戏？乙赞成。甲和乙找到一个奶茶店，说以后你们可以收比特币付账，收到的我回收，还付你一点手续费。奶茶店答应了。

下面甲乙开始玩游戏了：甲花一元钱买乙一个比特币，乙也花一元钱买甲一个比特币，现金交付；甲再花两元钱买乙一个比特币，乙也花两元钱买甲一个比特币，现金交付；甲再花三元钱买乙一个比特币，乙也花三元钱买甲一个比特币，现金交付……

于是在整个市场的人看来比特币的价格飞涨，不一会儿就涨到了每个比特币 60 元。但只要甲和乙手上的比特币数一样，那么谁都没有赚钱，谁也没有亏钱，但是他们重估以后的资产‘增值’了！甲乙拥有高出过去很多倍的‘财富’，他们身价提高了很多，‘市值’增加了很多。这个时候有路人丙，一周前路过交易平台的时候知道比特币是一元一个，现在发现是 60 元一个，他很惊讶。一个月以后，路人丙发现比特币已经是 100 元一个，他更惊讶了。他毫不犹豫地买了一个，因为他是个投资兼投机家，他确信比特币价格还会涨，价格上还有上升空间，因为据说有奶茶店开始接受比特币付款呢。而且自己也到奶茶店验证过，是真的。并且有人给出了超过 200 元的‘目标价’。

在甲、乙‘赚钱’的示范效应下，甚至路人丙赚钱的示范效应下，接下来的买比特币的路人越来越多，参与买卖的人也越来越多。比特币逐渐成为了一种大范围流通的数字货币。”

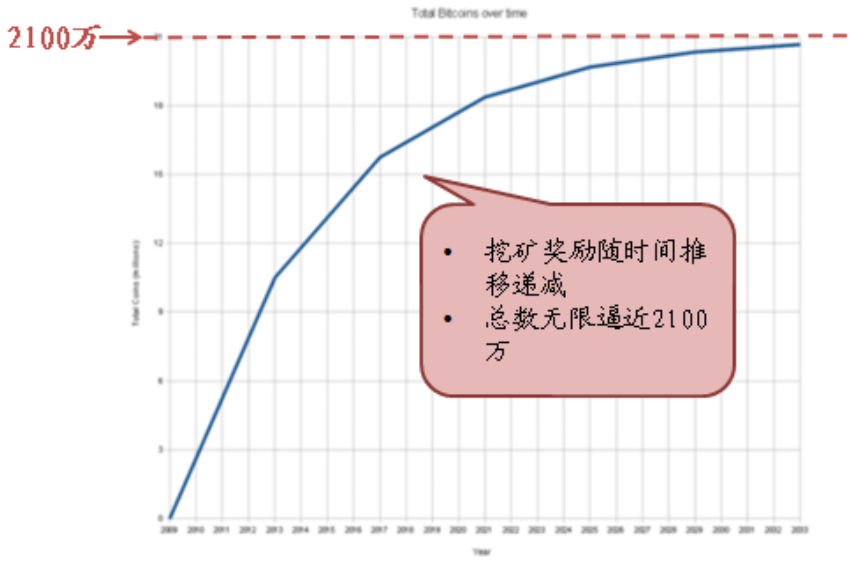
比特币的大致发展历程就如故事中所说，故事中的“神秘人”就是中本聪(Satoshi

Nakamoto)。2008 年，他在一个密码学讨论组上贴出了一篇研究报告，报告中阐述了他对一种电子货币的构想，比特币由此而来。

比特币的发行方式，靠用户自行“挖掘”发行：比特币的发行方式其实可以理解为解方程，方程有多重解，每当使用者解出了一组解，便可以获得一定数量的比特币，这种操作被形象地称为**“挖矿”**，比特币以这种被使用者“挖掘”的形式发行，当你找到了一个正确的解，你就好比挖到了一个金矿。这种发行方式使得每个“解题人”都可能成为比特币的发行方。在挖矿的过程中，当某人挖出一个未被发现的“解”时便向网络广播，网络中的节点验证其正确性，并在本地数据库进行查验，发现数据库中并无该解的记录，则确认该解的合法性并记录其持有人。

“谜？”——比特币的总数在设立之初便已确定：比特币的总数上限为 2100 万个，这取决于制造比特币的算法规则。简而言之，比特币的算法设计成随着挖矿参与人数上升，挖矿难度也随之上升的模式，最终使挖掘的时间基本恒定在每 10 分钟挖掘到一个“矿产”。最初，挖到矿之后奖励 50 个比特币，随着时间推移每隔 4 年奖励数减半，最终将在大约 2140 年逼近于 2100 万上限。至于算法的创造者当初为什么设定了 2100 万这个数字，依旧是个迷。

图 5：随着挖矿奖励的递减，比特币总数上限确定在 2100 万



资料来源：招商证券

比特币是否是庞氏骗局？尚无定论：近年来，关于比特币是否是庞氏骗局的讨论从未停息。比特币的反对者认为，比特币的早期挖掘者们占了很大的“便宜”，随着比特币被热炒，如果后续资金停止进入比特币市场，则比特币无法继续升值。对于老投资者的回报，只能依靠新投资者的加入来实现，这是一个金字塔形的利益体系，与庞氏骗局无异。而比特币的拥护者认为，庞氏骗局的特点是存在某个中心被围着转，后来者的钱会趋于流向这个中心，使其达到盈利的目的，而比特币却是去中心化的，它并不属于任何人或者任何组织，任何人都可以参与挖矿，后来者的钱并不会流向某个确定的群体。而之所以比特币价格一直飙高，是因为人们对它的未来抱有期望，而实际上比特币的使用范围也的确在增大，为人们提供跨国界、便捷的一种交易途径，这便是其价值的体现。

稀缺性强，比特币价格快速攀升：由于比特币的总数有限，加之随着挖矿难度的提升以及挖矿奖励的逐步递减，使比特币具有极强的稀缺性，前 4 年内全世界只有不超过 1050

万个，之后的总量将被永远限制在 2100 万个之内。比特币的价格从 2009 年诞生之初到近年实现了大幅攀升。在 2014 年一季度达到顶峰 4228 元人民币，截止 2016 年 2 月，比特币的人民币成交均价约为 2772 元。

图 6：比特币在中国成交均价走势图

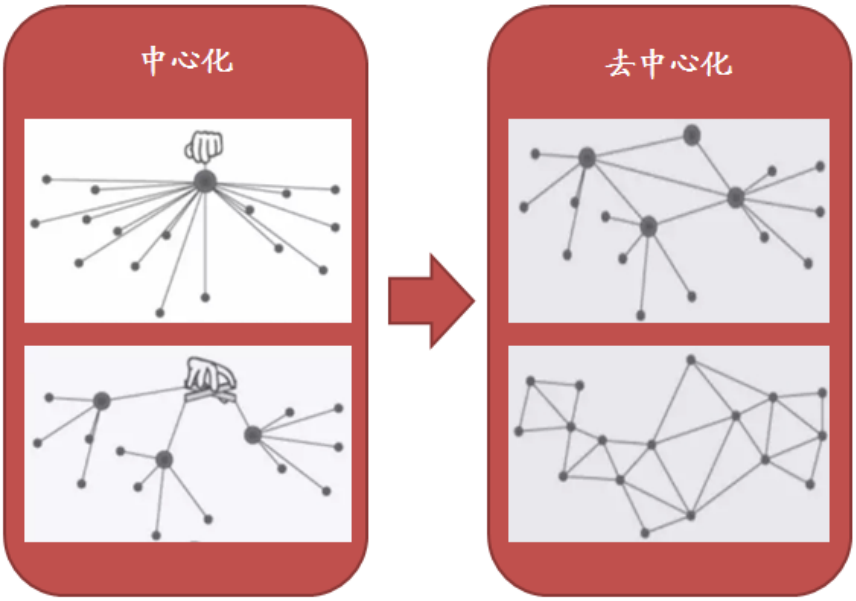
资料来源：Wind、招商证券

3、区块链：不完美的完美机制

区块链具有去中心化、去信任化、可扩展、匿名化、安全可靠等特点：

- **去中心化：**由于区块链是靠各个节点共同实现系统的维护和保证信息传递的真实性，基于分布式存储数据，而没有某个中心进行集中管理，因此某一个节点受到攻击和篡改不会影响整个网络的健康运作。

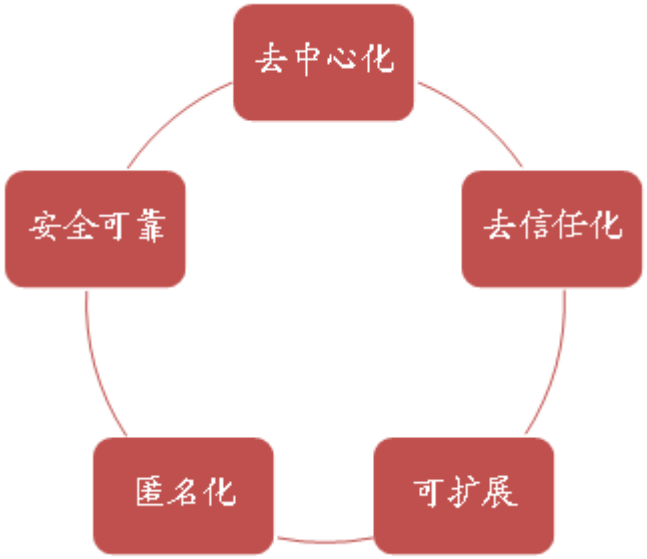
图 7：区块链的去中心化



资料来源：福布斯、招商证券

- **去信任化：**任意两个节点之间建立连接不需要信任彼此的身份，双方之间进行数据交换无需互相信任的基础。由于网络中的所有节点都可以扮演“监督者”的身份，因此不用担心欺诈的问题。
- **可扩展：**区块链是一种底层开源技术，在此基础上可以实现各类扩展和去中心化、去信任化的应用。
- **匿名化：**数据交换的双方可以是匿名的，网络中的节点无需知道彼此的身份和个人信息即可进行数据交换。
- **安全可靠：**由于任意节点之间的活动均受到全网的监督，并且数据库采用分布式存储，对于黑客来说，第一无法伪装和进行欺诈活动，第二无法仅靠攻克某个节点而控制网络。

图 8：区块链的特点



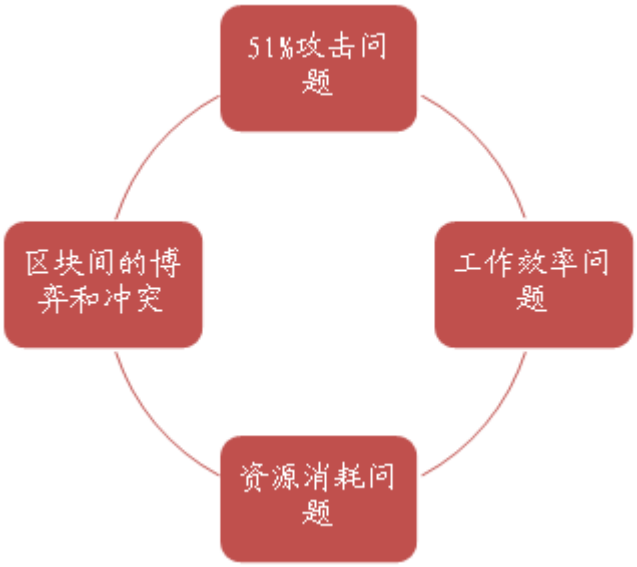
资料来源：招商证券

但是，区块链也存在着诸如 51%攻击的安全隐患、工作效率问题、资源消耗问题、区块间博弈和冲突等缺陷待解决。

- **51%攻击问题：**由于区块链的监管依靠网络中所有的节点共同完成，因此理论上说，如果掌握全网超过 51%的算力就有能力成功篡改和伪造区块链数据。
- **工作效率问题：**由于采用的分布式存储，区块链内的每个节点均需保存一份数据库，并且网络中发生的任何一笔交易其它节点均需进行认证并做记录，系统的工作效率较低，尤其在一些数据交换发生频繁的场景下区块链的应用性能会受限。因此如果想大规模推广并应用区块链技术，如何解决系统工作效率也将成为一个问题。
- **资源消耗问题：**由于去中心化容易引入资源的浪费，区块链的运作较为依赖网络节点贡献的算力，这些算力主要用于解决 SHA256 哈希和随机数搜索，除此之外并不产生实际社会价值，因而一般意义上认为这些算力资源是被“浪费”掉了，同时被浪费掉的还有大量的电力资源。因此如何解决区块链运作而带来的资源占用和浪费也将成为区块链大范围应用之前需要解决的问题。
- **区块间的博弈和冲突：**例如比特币中典型的“区块截留攻击”，它是由矿池的参与

者发起的攻击，对矿池和其它参与者的挖矿收益造成损害。发起区块截留攻击的矿工只向矿池发送部分工作量证明，但是如果他们发现了完整的证明，他们将抛弃该证明。因此矿池还是会向攻击者发放挖矿收益，但是矿池不能从攻击者的挖矿算力中受益。这减少了被攻击矿池的所有参与者的收益，当然也减少了攻击者自己的收益，攻击者们公平挖矿会获得更多的收益。因此如何设计激励相容的共识机制，提高系统内非法行为的成本，进而避免区块链的各节点在交互过程中发生博弈与冲突，也是区块链有待解决的缺陷之一。

图 9：区块链目前存在的缺陷



资料来源：《自动化学报》、招商证券

二、场景为王，关注央行数字货币

1、区块链：可应用场景非常广阔

我们认为比特币仅是冰山一角，区块链未来应用空间巨大：从理论上说，围绕区块链这套开源体系能够创造非常丰富的服务和产品。比特币只是区块链巨大应用空间的冰山一角。区块链技术将不仅仅能应用在货币体系中，还可以推演到各类社会服务、合约行为、交易行为中，诸如去中心化的微博、微信、搜索、租房，甚至是打车软件都有可能会出现。因为区块链将可以让人类无地域限制的、去信任的方式来进行大规模协作。纽约社会研究新学院哲学和经济理论家 Melanie Swan 在新书《区块链-新经济的蓝图》中指出，区块链的应用可能有 3 个阶段：

区块链 1.0：货币，即应用中与现金有关的加密数字货币,如货币、转账、汇款和数字支付系统等。

区块链 2.0：合约，如股票、债券、期货、贷款、智能资产和智能合约等更广泛的非货币应用。

区块链 3.0：在政府、健康、科学、文化和艺术方面有所应用。甚至最终实现去中心化自治社会的终极效果。

我们对区块链的可拓展的应用做一梳理，包括：**数字货币、支付清算、数字票据、权益证明、征信、政务服务、医疗等。**

图 10：区块链可能的应用

资料来源：招商证券

- **数字货币：**除了比特币，区块链在也有望应用于未来各国的法定数字货币之中。例如今年 1 月份，中国人民银行曾表示从 2014 年起就开始着手研究数字货币技术。今年 2 月央行行长周小川也曾表示央行的数字货币有可能采用区块链技术。

- **支付清算：**现阶段商业贸易交易清算支付都要借助于银行，这种传统的通过中介进行交易的方式要经过开户行、对手行、央行、境外银行（代理行或本行境外分支机构）。在此过程中每一个机构都有自己的账务系统，彼此之间需要建立代理关系，需要有授信额度；每笔交易需要在本银行记录，还要与交易对手进行清算和对账等，导致交易速度慢，成本高。与传统支付体系相比，区块链支付为交易双方直接进行，不涉及中间机构，即使部分网络瘫痪也不影响整个系统运行。如果基于区块链技术构建一套通用的分布式银行间金融交易协议，为用户提供跨境、任意币种实时支付清算服务，则跨境支付将会变得便捷和成本低廉。区块链技术在支付清算上的应用并非遥不可及，SWIFT 作为一个链接了数万家银行的通信平台，已经被新兴崛起的区块链技术所威胁，一些区块链初创企业和合作机构开始提出一些全新的结算标准，如 R3 区块链联盟已经制定了可交互结算的标准，截至目前全球已有 42 家大型银行和金融集团加入 R3。

- **数字票据：**数字票据是结合区块链技术和票据属性、法规、市场，开发出的一种全新的票据展现形式，与现有的电子票据体系的技术架构完全不同。数字票据既具备电子票据的所有功能和优点，又融合了区块链技术的优势，成为了一种更安全、更智能、更便捷、更具前景的票据形态。数字票据的核心优势主要表现在：1）实现

票据价值传递的去中介化。在传统票据交易中，往往票据中介利用信息差进行撮合，借助区块链实现点对点交易后，票据中介将失去中介职能，重新进行身份定位。2）有效防范票据市场风险。区块链由于具有不可篡改的时间戳和全网公开的特性，一旦交易，将不会存在赖账现象，从而避免了纸票“一票多卖”、电票打款背书不同步的问题。三是系统的搭建和数据存储不需要中心服务器，省去了中心应用和接入系统的开发成本，降低了传统模式下系统的维护和优化成本，减少了系统中心化带来的风险。四是规范市场秩序，降低监管成本。区块链数据前后相连构成的不可篡改的时间戳，使得监管的调阅成本大大降低，完全透明的数据管理体系提供了可信任的追溯途径，并且可以在链条中针对监管规则通过编程建立共用约束代码，实现监管政策全覆盖和硬控制。

- **权益证明：**区块链每个参与维护节点都能获得一份完整的数据记录，利用区块链可靠和集体维护的特点，可对权益的所有者确权，可应用于各类金融产品的交易。对于存储永久性记录的需求，区块链是理想解决方案，适用于土地所有权、股权交易等场景。其中股权证明是目前尝试应用最多的领域，股权所有者凭借私钥，可证明对该股权的所有权，股权转让时通过区块链系统转让给下家，产权明晰，记录明确。整个过程无需第三方的参与。在伦敦举办的 2015 年欧洲卓越贸易技术金融新闻奖的主题演讲中，纳斯达克首席执行官 Bob Greifeld 宣布，该交易所打算使用区块链技术管理代理投票系统。代理投票本来是由一家上市交易所使用的一项重要而又费时的操作，区块链技术的应用可以让股东们不必出席公司周年大会就能参与投票，人们用自己的手机就能投票，并且永远保存投票记录。区块链技术被视为股权交易领域能够在更短时间内确保透明交易的先进技术。

- **征信：**目前，商业银行信贷业务的开展，无论是针对企业还是个人，最基础的考量是借款主体本身所具备的金融信用。各家银行将每个借款主体的还款情况上传至央行的征信中心，需要查询时，在客户授权的前提下，再从央行征信中心下载参考。这其中存在信息不完整、数据不准确、使用效率低、使用成本高等问题。在这一领域，区块链的优势在于依靠程序算法自动记录海量信息，并存储在区块链网络的每一台计算机上，信息透明、篡改难度高、使用成本低。各商业银行以加密的形式存储并共享客户在本机构的信用状况，客户申请贷款时不必再到央行申请查询征信，即去中心化，贷款机构通过调取区块链的相应信息数据即可完成全部征信工作。

- **政务服务：**区块链另一个重要应用在于政府职能领域，即通过区块链技术，以分布式、高效、低成本的方式提供政务服务。通过采用区块链去中心化的特点，成为一个无国界的分布式账簿，包含了社会的文档、记录及其使用历史，同时区块链政务服务的提供将建立在一个强大的个人信息系统基础之上，系统中包含信用、纠纷记录、投票、国民收入、法律文件（如土地契约、医嘱、育儿合同、婚姻合同等）。由于区块链具有不可篡改性，婚姻将是极佳的应用场景，因为它意味着一对夫妻将把他们的婚姻永远连接在一个共享的储存账户上（例如比特币钱包）。世界上第一个用区块链记录的婚姻发生在佛罗里达的迪士尼乐园里，这个婚礼被提交到比特币的区块链里，这对夫妇的誓言被传输成文档注释，并嵌入到一笔 0.1 个比特币的交易当中，从而永久的保存在区块链的分类账中。

图 11：世界第一个应用区块链的婚姻

资料来源：《Blockchain-Blueprint for a new economy》、招商证券

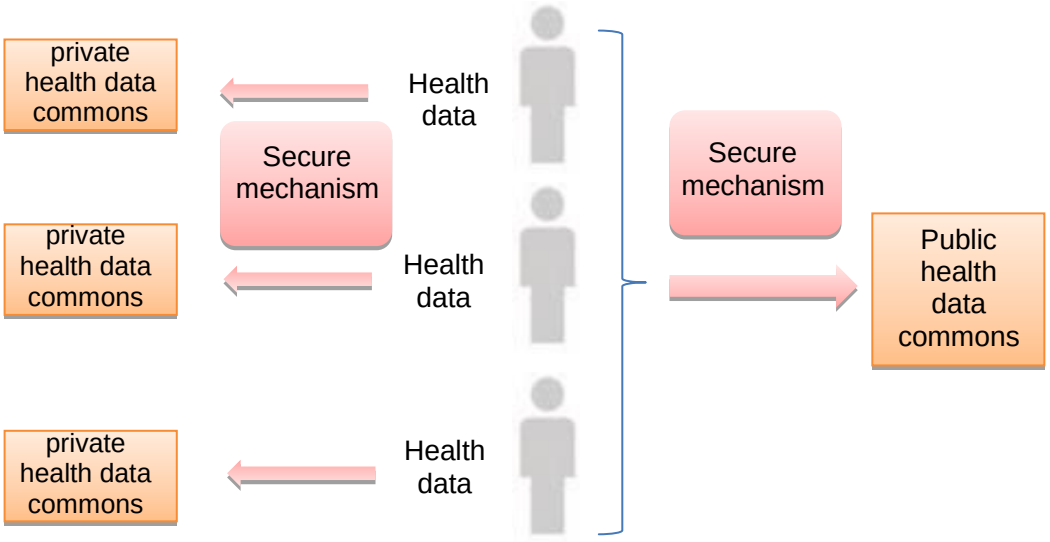
基于区块链的政务服务同时给予市民完全的自主权。就像比特币作为一个更好的货币出现一样，同样的情况也会在政府服务领域出现，同样的传统政府服务将会因为区块链技术的使用而变得更加低成本、去中心化以及更加定制化。同时所有的政府法律文件，如合同、身份证明都能够被储存在区块链中。而例如区块链护照之类的基于区块链技术的个人身份系统，需要得到相当多数人的接受才能够被公众所承认，正如比特币当时一样，需要被许多人认同才能够被广泛地应用为货币。目前一个叫做 World Citizen project 的项目正在提供区块链护照系统，致力于创造一个适用于全球的市民体系，并已经采用加密工具设计了区块链护照。

图 12：World Citizen project 的区块链护照

资料来源：《Blockchain-Blueprint for a new economy》、招商证券

- **医疗健康领域：**区块链能够给医疗健康领域带了的主要益处在于，能够使得健康数据被大范围分析的同时保持了数据的隐秘性：1）利用区块链技术的匿名性特征，个人的健康数据能够被编码成为一笔数据资产，并像数字货币一样被放入区块链中，个人能够通过手中的私人钥将数字医疗资产授权给医生、保险机构、药店等使用。这种将电子医疗记录信息系统放到区块链的服务，能够解决原来大医疗机构的数据无法共享的问题。2）另一个益处在于区块链遵守统一的规范和准则，提供一个标准的安全机制，所有的健康数据都在统一的规范下转换可供研究的数据模式。由于这种数据资产是统一的，因此几乎所有的医疗数据储存点都能够进行分析。

图 13：区块链将健康信息数字化



资料来源：《Blockchain-Blueprint for a new economy》、招商证券

2、央行数字货币：可能采用区块链技术

2016 年 1 月 20 日，中国人民银行数字货币研讨会召开，并表示从 2014 年起就成立了专门的研究团队研究数字货币技术。2016 年 2 月 15 日，央行行长周小川接受采访，再次传递了**三个关于央行数字货币的重要信息**：

1）未来数字货币与现金将在长时间内并行、逐步替代；

2）数字货币将作为法定货币，由央行发行并保障其安全性；

3）央行的数字货币有可能采用区块链技术，已部署重要力量探讨其应用。

2.1、央行数字货币 VS 比特币

比特币难成为法定货币：虽然有诸多颠覆性的优点，比特币也存在着交易效率低、价格波动大、交易平台安全性有待提高、缺少政策支持等问题：

- **交易效率低：**比特币客户端在安装的时候，需要花大量时间下载一个包括所有历史交易信息的数据包，在此之后，每一次交易的确认时间长达 50 分钟，影响交易效率。
- **价格波动大：**剧烈的价格波动不利于比特币成为一种流通货币，而更像是一种投机

商品。

- **交易平台安全性有待提高：**由于比特币的交易往往是通过一些网站平台达成，许多用户直接使用本地货币购买比特币，因此这些交易平台往往易受黑客攻击。
- **缺少政策支持：**虽然比特币的流通范围很广，但毕竟不是法定货币，是否接受比特币支付完全取决于个人对其价值的期望。且目前大部分国家对比特币的态度不明朗，比特币在美国被政府归类为一种商品而非货币，归于商品交易法案的管辖之内；德国是对比特币相对开明的国家，把比特币定义为一种货币单位和私有资产。在我国，银行与金融机构被禁止从事与比特币相关的交易，但是并不限制普通公民交易或挖掘比特币。

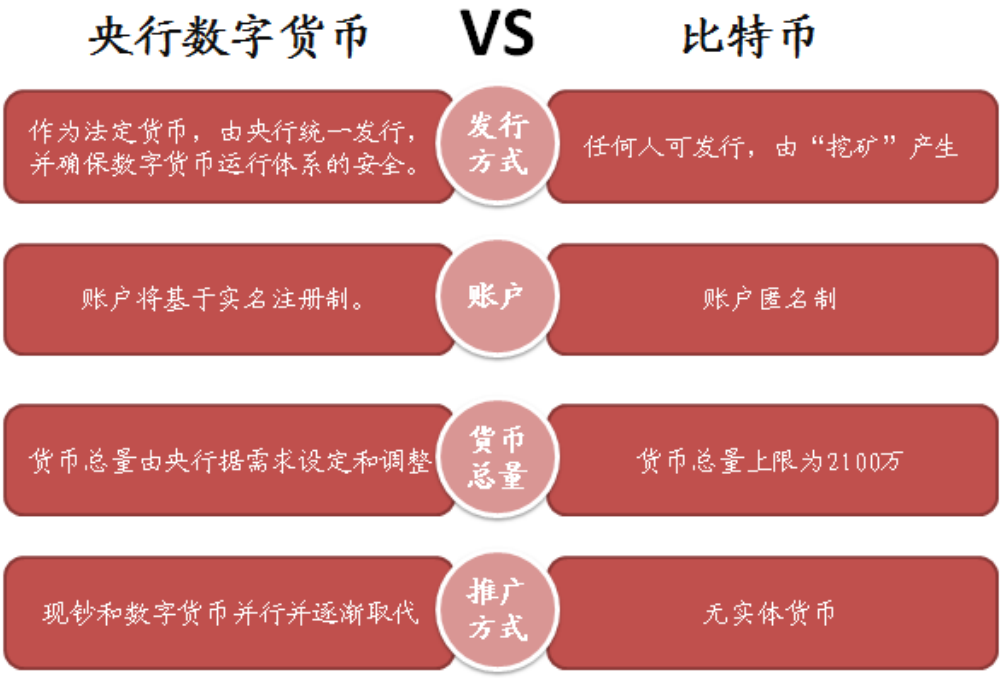
图 14：比特币存在的问题

资料来源：招商证券

央行数字货币≠比特币：比特币与央行数字货币同属数字货币，但是比特币不等于央行数字货币。比特币只是若干数字货币中的一种，至今人们说起数字货币，往往第一反应就是比特币，那是因为比特币是目前为止最成功的数字货币。而央行的数字货币虽然有可能会借鉴比特币的区块链技术，但在很多方面将和比特币有很大的不同：

- **货币发行方式：**不同于比特币的“挖矿”机制，央行数字货币将作为法定货币，由央行统一发行，并确保数字货币运行体系的安全。
- **实名制：**不同于比特币账户的匿名化交易，央行数字货币的账户将基于实名注册制。
- **货币总量：**比特币的货币总量设定为 2100 万。而对于国家级货币来说，这个数量显然是远远不够的。央行数字货币的总量可由央行根据需求进行调整。
- **现钞和数字货币并行：**央行数字货币将采取现钞和数字货币并行并逐渐过度的形式。现钞的发行和回笼是基于现行“中央银行—商业银行机构”的二元体系来完成的。而数字货币的发行过度阶段或许将仍然基于该二元体系完成。

图 15：央行数字货币与比特币对比

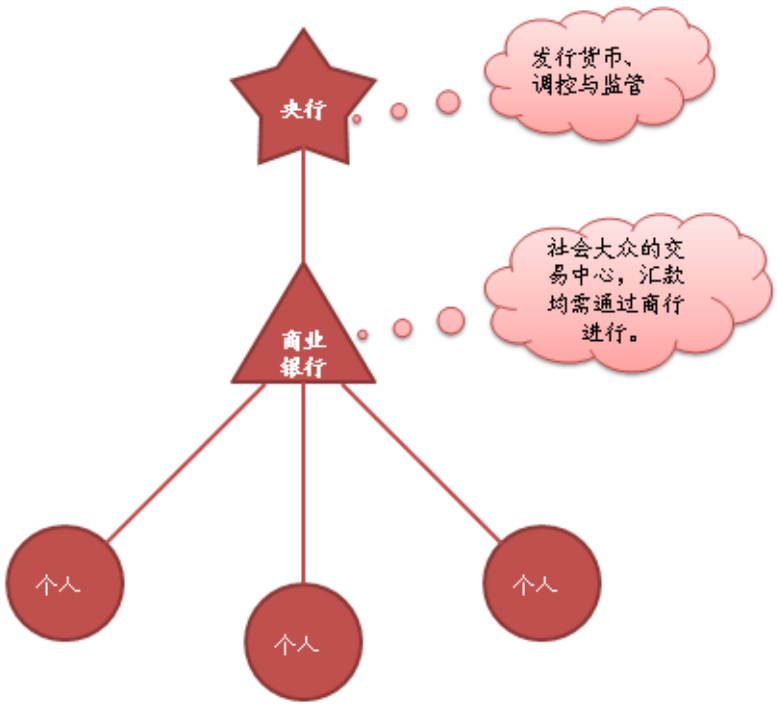


资料来源：招商证券

2.2、央行数字货币落地形式大猜想

传统货币运作形式：传统的货币流通形式是通过央行统一发行，然后由商业银行机构起到央行和市场间桥梁的作用，而市场中的个人与机构都是通过商业银行作为“中间人”进行交易。

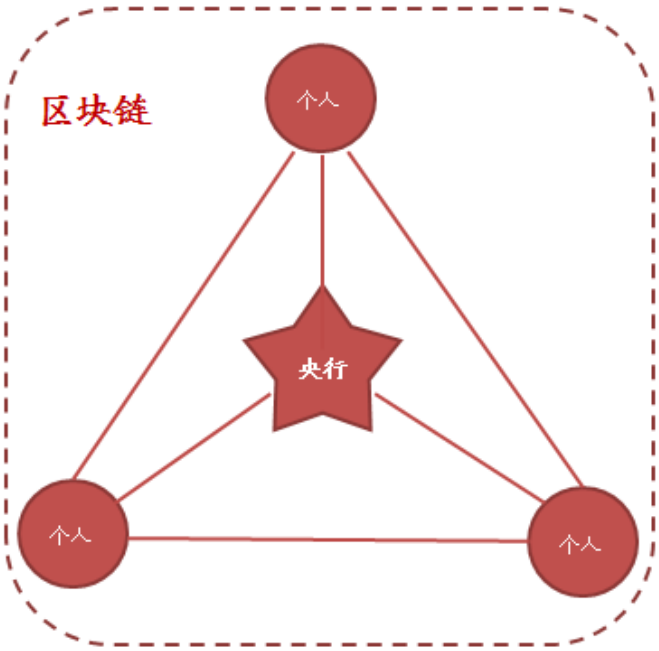
图 16：传统货币的运作模式



资料来源：招商证券

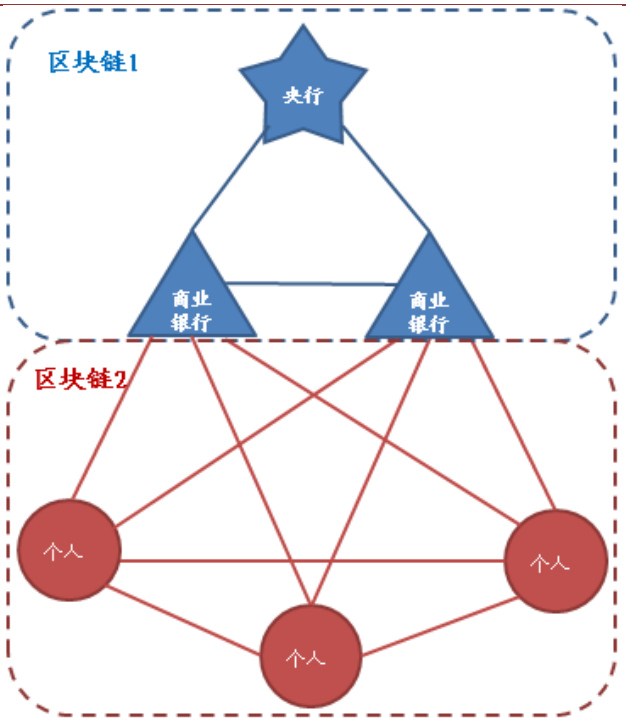
我们对央行数字货币的“猜想”：如果央行数字货币借鉴区块链技术来实现，我们猜想其最终的呈现形式可能有两个方向：1）一是逐渐过渡直到最终摒弃传统的“中央银行—商业银行机构”的二元体系，央行以一个节点的形式加入到区块链网络中直接提供货币发行和监管，商业银行机构的角色将不再存在。2）二是依旧保留“中央银行—商业银行机构”的二元体系，商业银行机构将接入区块链，共同起到参与市场运作的作用，而央行也将与各商业银行机构连接，并通过区块链技术实现央行与商行、商行与商行之间的监督与信息传递。在这种模式下，我们认为央行和社会个体的连接模式可以是（a）类似于去二元体系下的情况，央行直接参与市场活动，与社会个体保持连接，也可以是（b）央行与商行形成区块链 1，商行与个人形成区块链 2，两个区块链相连，在必要的时候央行可以启动两个区块链的连接并直接作用于社会个体。（a）（b）两种情况其实是殊途同归的，但（b）具有相对更高的灵活性且具有较低的建设和管理成本，同时央行在其中还具备很强的调控能力，因此我们认为呈现（a）的可能性不大。

图 17：央行数字货币的可能落地形式 1



资料来源：招商证券

图 18：央行数字货币的可能落地形式 2



资料来源：招商证券

2.3、数字货币将为央行带来长远的积极影响

若发行央行数字货币，将带来降低成本、打击犯罪、以及帮助央行更好进行货币调控等诸多长远性积极影响：

1) **降低传统纸币发行、流通、损毁等成本：**参考美联储对于美元的统计信息，非聚酯美元钞票按面额分类的平均生命周期仅为 6.9 年，硬币的平均生命周期为 25 年，一旦纸币达到使用期限，将被回收粉碎并压成砖块，送到政府指定焚化炉去烧毁。根据 Hass McCook 在《货币成本》中的估算，2014 年世界上至少有 2000 亿张钞票和 1.5 万亿枚硬币在流通，而这些实体货币的流通会对环境产生一定影响，包括纸张生产和印刷过程中水消耗、废墨水和纸浆污泥、印刷和纸浆制造用电、金属采矿及铸币等，进而估算得到全球因纸币的使用共产生 1840 万吉焦，即大约 307 万

吨二氧化碳，因铸造硬币共产生 2125 万吉焦，即约 350 万吨二氧化碳。实体货币对环境造成的影响一进步提高了实体货币的使用成本。

表 1：美元纸币生命周期

美元纸币面额	生命周期（年）
1	5.9
5	4.9
10	4.2
20	7.7
50	3.7
100	15.0

资料来源：美联储、招商证券

2) **提高监控力度，减少违法犯罪行为：**区块链的运作机制使交易过程透明公开化，有利于对经济活动进行监管，减少洗钱、交易欺诈、盗窃、黑市交易、逃漏税等违法犯罪行为。纸币易被伪造且容易发生洗钱行为，难被追踪。区块链技术使每一笔钱可以从诞生一直追溯到最后的拥有者，可以有效提高资金追踪能力。此外，据统计每年约有 1.4%的零售收入损失在盗窃行为上，而实体货币的消失也杜绝了盗窃货币现象的发生。

图 19：可使用自动化工具完成区块链上的资金流向分析

资料来源：比特币资讯、招商证券

3) **有利于央行更好地调控货币的供应与流动性：**在传统的货币供给模式中，央行的大部分货币调控工具只能通过影响银行来间接调控市场，这样一是会引起从政策下放到最终体现效用上的延时，二是可能会存在调控政策落实不到位，曲解央行本意的情况。通过数字货币，央行可以随时跟踪货币的流向，做到动态应对。甚至可以直接将钱打到目标群体的手上，将货币调控效率发挥到最大化。

三、国外区块链发展与案例

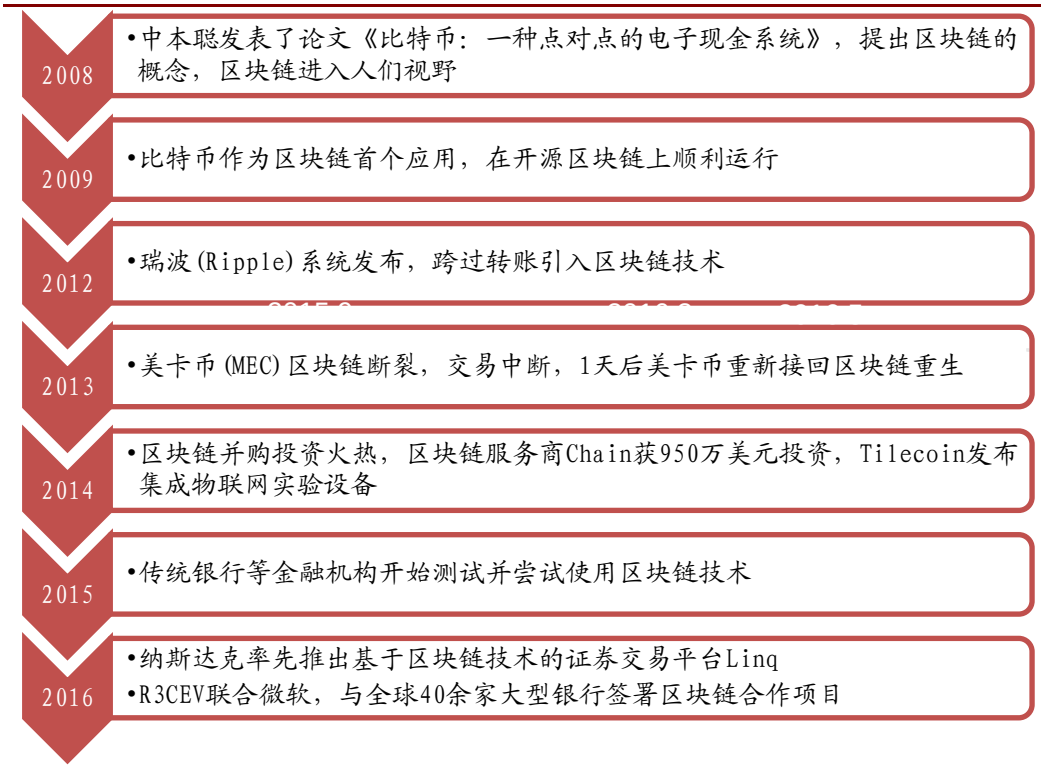
区块链在国内虽然还处于概念导入和探索的初期阶段，但国际上许多大型银行以各种形式在区块链领域已经开展了一系列探索，我们归纳来看主要有三种途径：

a) 一是商业银行成立内部的区块链实验室。比如花旗银行、瑞银、纽约梅隆银行等已相继成立研发实验室，重点围绕支付、数字货币和结算模式等方面测试区块链的应用，有的还扩大到其员工内部系统中测试。

b) 二是投资金融科技初创公司。2015 年以来，许多跨国大型金融集团纷纷以创投形式进入区块链领域，比如高盛联手其他投资公司向比特币公司 Circle 注资 5000 万美金，西班牙对外银行通过旗下子公司以股权创投方式参与了 Coinbase 的 C 轮融资等。

c) 三是与初创公司合作。例如巴克莱银行在技术孵化和加速器项目中与区块链初创公司合作，澳大利亚联邦银行和开源软件 Ripple 合作组队，创建了一个在其子公司之间互相支付转账的区块链系统等。

图 20：国际上区块链发展大事记



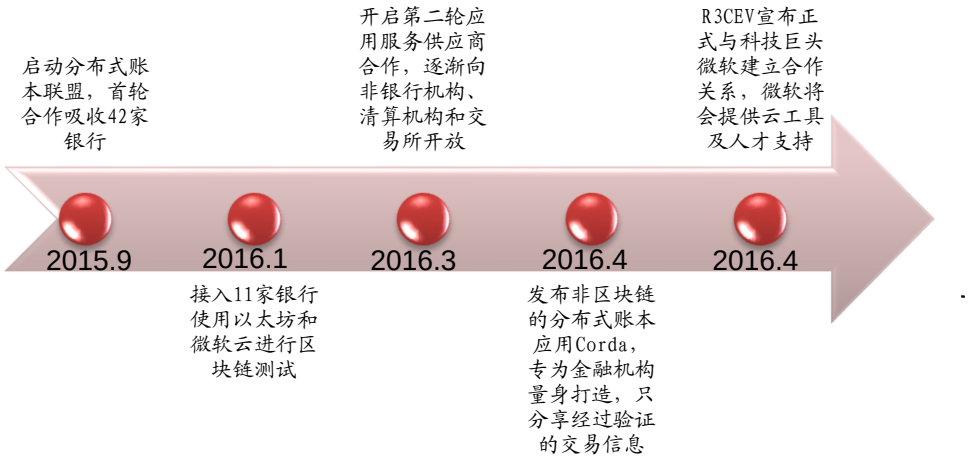
资料来源：招商证券

1、案例一——R3CEV

全球最大的区块链 R3CEV： R3CEV 是由摩根大通、高盛等 42 家国际银行组成，与科技巨头微软合作。自 2015 年启动以来，进展速度非常快：在首轮合作中吸引了巴克莱、瑞士信贷、汇丰等 42 家金融机构。2016 年 1 月，11 位 R3 联盟成员完成了使用微软区块链服务平台（BaaS）的以太坊网络私人版本的测试，之后 R3CEV 开始着手于与微软建立合作关系。2016 年 4 月，R3 宣布了非区块链的分布式账本应用 Corda，具有

区别于区块链的特征，Corda 拒绝了原来区块链把所有数据拷贝给所有参与者的概念，只有经过验证的交易信息才可以分享，这一点与在节点中分布全部交易历史的区块链是不同的，并给监管机构提供“监管观察员节点”，可以从这个节点监控系统运作。包括 Overstock 的 t0 平台也在区块链系统中搭建这个功能。

图 21：R3 成立以来进展迅速

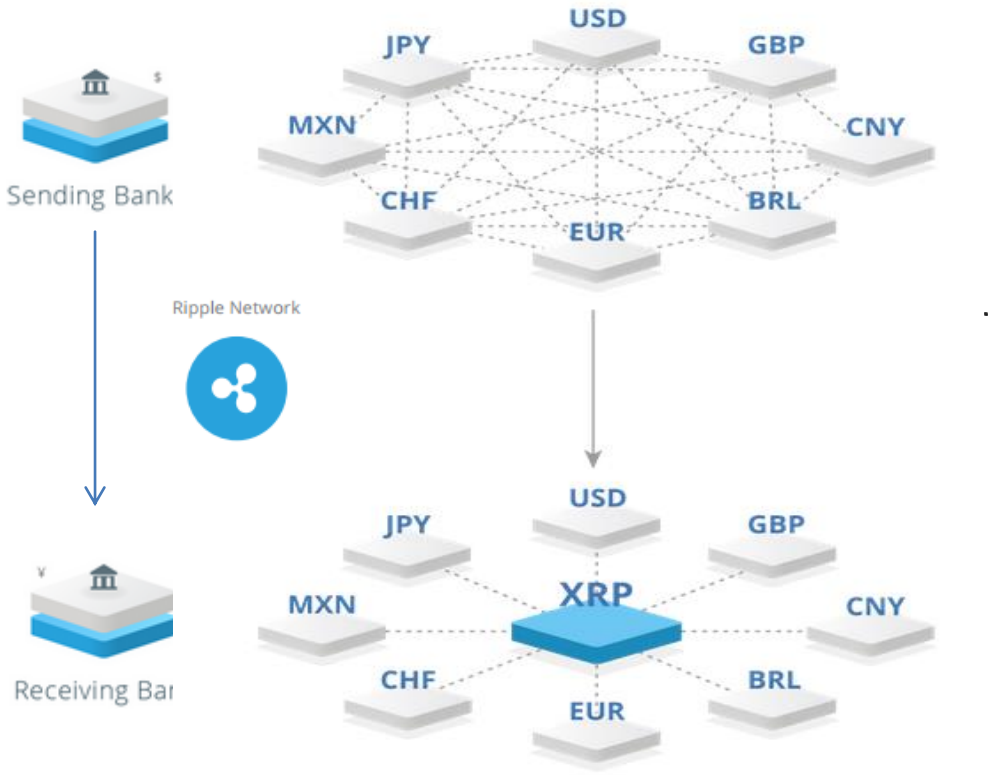


资料来源：比特资讯、招商证券

2、案例二——Ripple

世界上第一个开放的支付网络 Ripple： Ripple 定位为全球金融解决方案，它的商业模式是直接提供给银行类金融机构汇款技术和底层协议，通过其建立的基于 XRP 的支付网络，让世界各地的银行可以直接交易任意一种货币，包括美元、欧元、人民币或者比特币，而无需中央对手方或代理银行。这相当于替换原来成本高昂的 SWIFT 技术，为银行削减成本。

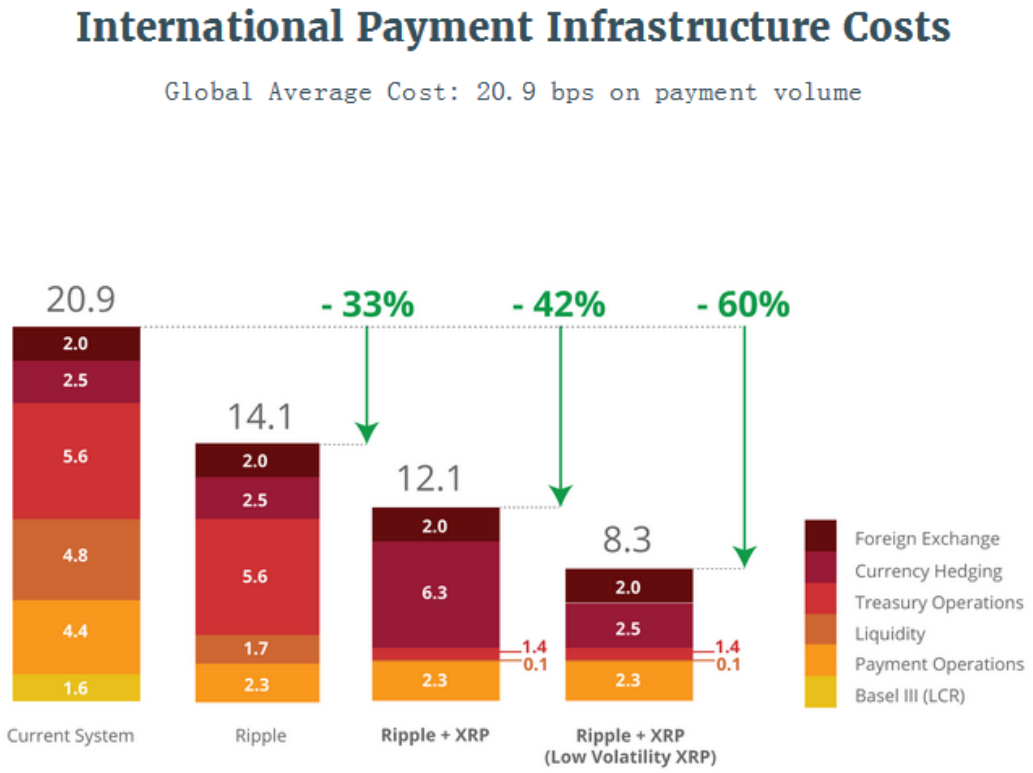
图 22：Ripple 商业模式



资料来源：Ripple 官网、招商证券

Ripple 具有压倒性的成本优势：2016 年 2 月，使用 Ripple 网络及本机加密代币 XRP（瑞波币）进行跨境支付的银行与使用传统的银行跨境支付相比可节约多达 42％的费用，同时 Ripple 表示如果受访银行在进行国际支付时使用 Ripple 网络（不使用 XRP）则可节省 33％的费用，流动性成本减少 65％，支付运营成本减少 48％，并且 Basel III 税务执行费用也会减少 99％。

图 23：Ripple 具备的成本优势

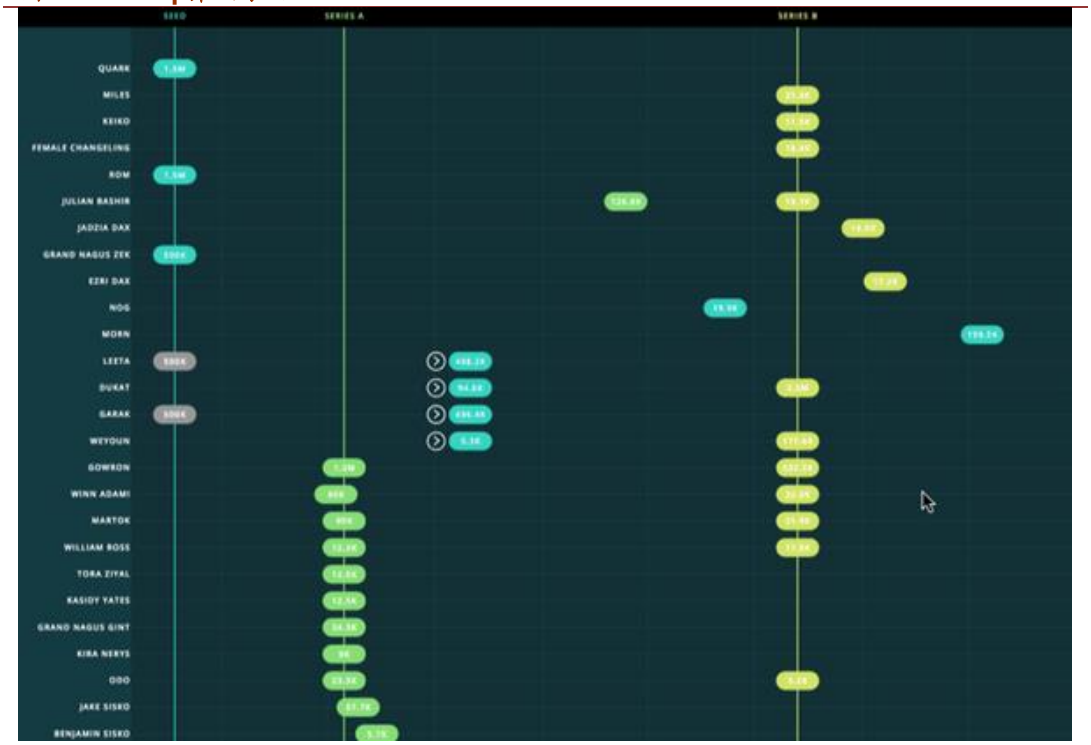


资料来源：Ripple 官网、招商证券

3、案例三——Linq

区块链技术的私人股权市场 Linq：纳斯达克在 2015 年 10 月正式推出了它的区块链平台 Nasdaq Linq。通过 Nasdaq Linq 发行股票的发行者享有一种“数字化”的所有权。通过区块链交易，Linq 极大地加速了公开市场的交易结算，使原本股权交易市场标准结算时间从 3 天提升到十分钟，使结算风险降低 99%，从而有效降低资金成本和系统性风险；Linq 还有效简化了交易双方在线完成发行和申购材料的多余文字工作，同时降低发行者因繁重的审批流程所面临的行政风险和负担。Chain 是第一家使用 Linq 技术发行公司股票的公司，上市公司的所有股份数字，包括尚未分配的股份，都通过可视化的颜色块来代表，纳斯达克称该数据为“股权时间轴视图”。那些已经发生的交易将会在时间轴上显示为“空”，并且变成灰色。用户还可以看到箭头，说明该股份是如何被转移和划分的。

图 24：Linq 界面展示



资料来源：互联网、招商证券

4、案例四——Hyperledger

超级账本项目 Hyperledger：Hyperledger 是由 Linux 基金会联合全球超过 40 家金融、科技及区块链技术团队，致力于加速推动分散式分类帐技术的开源区块链专案，通过为企业级的开源分布式账本创建一种跨行业开放标准，让自由开发人员专注于建设强大的特定行业应用、平台和硬件系统，实现几乎所有的数字价值交换，如房地产合约，能源交易和婚姻证书，都能够被安全且高效地跟踪和交易。2016 年 4 月，Hyperledger 完成了关键领导岗位的部署，成立了 11 个组织组成的技术指导委员会，由 IBM 出任主席，埃森哲、因特尔、区块链联盟 R3、CME Group 等 10 个组织任技术指导委员，将主导接下来的整个开源区块链技术发展方向，确保讨论、开展与决策的过程皆开放且透明，并负责评估、管理所有贡献至专案的程式码，藉由开放社群的流程，建立出一套初期且统一的底层程式码。

图 25：Hyperledger 成员组成

资料来源：Hyperledger、招商证券

投资建议：

目前，区块链虽然在国内还处于概念导入期和研究应用的初期阶段，但我们已经看到国外一些机构和组织已快速布局相关领域，比如在金融领域，比如高盛、摩根大通等大投行组建了区块链联盟 R3 推广区块链在银行领域的应用；纳斯达克在去年 10 月正式推出区块链平台 Nasdaq Linq，且成功的应用区块链发行了第一家公司：Chain 的股票。除了金融领域，我们也看到在一些个别地区和机构当中，区块链已应用在结婚登记和护照系统等诸多领域。

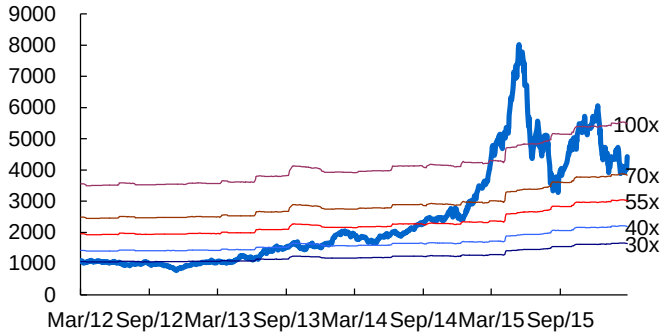
我们认为区块链更类似于一种新的协议机制，这种机制有望打破原有的中心化数据库模式，将数据通过分布式记录和存储的方式留在每个个体当中，从而改变数据的价值提取方式。这样一来，区块链甚至有望彻底颠覆现有的中心化 IT 模式，使得现有的互联网架构重新洗牌，传统的 IT 厂商有望借助区块链的大浪潮得到重新分配蛋糕的机会。我们建议投资者关注拥有区块链开发能力和应用能力的 IT 厂商，建议关注：1）金融 IT 领域的：**恒生电子、赢时胜、海立美达、信雅达、金证股份、广电运通**；2）加解密相关标的：**卫士通、飞天诚信**。

风险提示：

1、区块链短期内还不具备大规模推广应用的条件，短期不会对相关标的产生盈利影响。

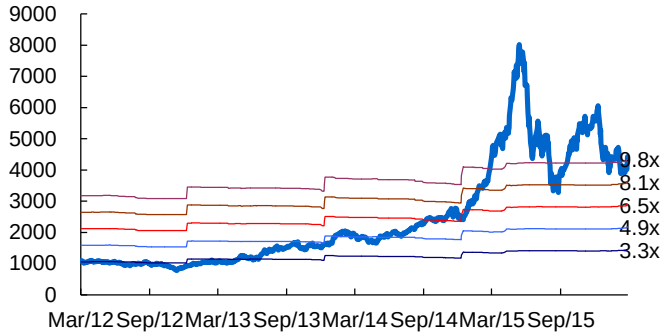
2、区块链目前还处于研究应用早期阶段，标准还未形成。

图 26：计算机行业历史PEBand



资料来源：贝格数据、招商证券

图 27：计算机行业历史PBBand



资料来源：贝格数据、招商证券

参考报告：

1、《比特币基础科普与常见误解》2015/10

2、《Blockchain-Blueprint for a new economy》2015/01

分析师承诺

负责本研究报告的每一位证券分析师，在此申明，本报告清晰、准确地反映了分析师本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与，未来也将不会与本报告中的具体推荐或观点直接或间接相关。

刘泽晶：2014/15 年新财富计算机行业团队第三、第五名，2014 年水晶球团队第三名。中央财经大学硕士毕业，6 年从业经验。

黄斐玉：招商证券计算机行业分析师，北京航空航天大学硕士。具有摩托罗拉、联想集团等 IT 公司产品研发，技术预研等领域多年工作经验。

徐文杰：招商证券计算机行业分析师，北京航空航天大学硕士。曾供职于 IBM， VMware 等公司从事大数据、云计算领域的工作。

感谢招商证券计算机团队宋兴未对本文做出的杰出贡献!

投资评级定义

公司短期评级

以报告日起 6 个月内，公司股价相对同期市场基准（沪深 300 指数）的表现为标准:

强烈推荐：公司股价涨幅超基准指数 20%以上
审慎推荐：公司股价涨幅超基准指数 5-20%之间
中性：公司股价变动幅度相对基准指数介于±5%之间
回避：公司股价表现弱于基准指数 5%以上

公司长期评级

A：公司长期竞争力高于行业平均水平
B：公司长期竞争力与行业平均水平一致
C：公司长期竞争力低于行业平均水平

行业投资评级

以报告日起 6 个月内，行业指数相对于同期市场基准（沪深 300 指数）的表现为标准:

推荐：行业基本面向好，行业指数将跑赢基准指数
中性：行业基本面稳定，行业指数跟随基准指数
回避：行业基本面向淡，行业指数将跑输基准指数

重要声明