证券研究报告—深度报告

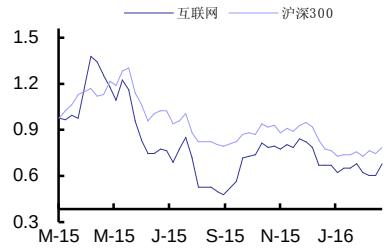
互联网

区块链专题研究

无评级

2016 年 03 月 21 日

一年该行业与沪深 300 走势比较



相关研究报告:

《互联网行业周报：企业微信即将发布，企业级服务竞争升级》 ——2016-03-14

《互联网行业周报：B2C 电商强劲增长，微博用户突破 2.3 亿》 ——2016-03-08

《京东（JD）：Q4：收入维持强劲增长》 ——2016-03-04

《互联网行业周报：中概股季报频出，业绩增长显著》 ——2016-03-02

《百度（BIDU）：剥离去哪儿后财报超预期》 ——2016-02-29

证券分析师：王学恒

电话：010-88005382

E-MAIL：wangxueh@guosen.com.cn

证券投资咨询执业资格证书编码：S0980514030002

联系人：何立中

电话：010-88005322

E-MAIL：helz@guosen.com.cn

独立性声明:

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

行业专题

区块链:可代替 VISA 的低熵新网络

- **核心思想：分布、共享、不可篡改**

区块链是一种创新的分布式交易验证和数据共享技术，也被称为分布式共享总账。通过构建点对点组织网络、时间有序不可篡改的密码学账本、分布式共识机制，实现去中心化信任。两种意义：一是支撑比特币系统的一系列技术。二是将区块链技术作为灵感以用来解决金融与其他行业存在的一些问题。

- **三步走理解区块链技术原理**

技术原理分 3 步走：1.把一段时间内的信息打包成一个区块（赋一随机序列）；2.盖上时间戳（用随机序列生成一个哈希值）；3.与上一个区块衔接在一起，形成新的区块。改变区块链中任何一处数据最终会引起全区块链反应。

- **牵一发而动全身：密码学中的哈希函数保证了数据不能篡改**

非对称加密算法信息发送流程既证明信息是 A 发出的，又能保证只有 B 才能解密。**私钥加密数据，用公钥能解密，但是用公钥加密信息只有私钥解得开。**密码学的哈希函数有三大性质：**1.找不到两个不相等的值 x 和 y 使得 H（x）= H（y）；2.由哈希函数 y=H（x）的输出结果 y 从得不到输入值 x，在计算上是不可行的。3.通俗讲就是：求解哈希函数只能用穷举法一个一个去试，不能直接求解。**

- **第五次颠覆性的新计算范式**

从计算范式看现代社会进化过程，每隔 10 年就会有一次新的范式出现。大型机、个人电脑范式、互联网、移动终端、社交网络。接下来是 10 年，基于区块链加密协议的网络很有可能就是新的范式。到 2016 年 3 月 18 日，比特币区块链上共有 403219 个区块，数据总容量 43GB，全网算力在 1000PFLOPS（每秒 1000 万亿次浮点计算），这些计算能力由全球接入比特币系统的计算机免费提供。目前我国的天河二号超级计算机的算力也只有 34 PFLOPS。

- **公开的分布式账本代替 VISA 清算**

分布式共享式账本分布于全网算力节点之上，而执行交易的权利是由密码学设置的公私钥来决定的。通过共享注册表记录所有权的网络结构。相比于现在的交易网络，分散式分类账取消了清算中心进行点对点自我清算。

- **能够降低熵，创造一种新的网络组织**

世界人口的增长带动能源需求的增长，在能源无法满足人类需求情况下，从物理学角度看，改变发展模式来降低熵的增加，区块链提供了另外一种发展模式。类似蜜蜂筑巢式分布式管理增加有序降低熵，分布网点越多，熵降低的可能性越大，中国网名数世界第一，具有降低熵的基础优势。（注：熵是一个系统中“无秩序”的程度，也表征生命活动过程质量的一种度量）

- **投资建议**

已经有很多金融机构尝试使用区块链解决日常复杂、高成本的业务。央行也开始研究区块链，但是现阶段还处于初期，距大规模应用，未来还有很长路遥走。从二级市场投资角度看，A 股以及海外上市公司都没有区块链标的，该领域的创新和应用还在一级市场。从相关性上来看，A 股的一些安全概念股（涉及到密码）、征信概念股（未来信用）、大数据概念股（数据区块连接）。

内容目录

图表目录

分布、共享、不可篡改

区块链（Blockchain）是一种创新的分布式交易验证和数据共享技术，也被称为分布式共享总账（Distributed Shared Ledger）。区块链的核心价值在于，通过构建 P2P 自组织网络、时间有序不可篡改的密码学账本、分布式共识机制，从而实现去中心化信任（Decentralized Trust）。

一个区块简单来说就是一系列支付的列表。区块链就是一系列区块链的列表，每一个区块链都可以追溯到前一个区块。 **然而，当人们在讨论区块链的时候，区块链一般指的是支撑比特币系统的一系列技术。其他的一些项目将区块链技术作为他们的灵感以用来解决金融与其他行业存在的一些问题。**

区块链是一本全网记录所有已发生的交易的公开的分布式账本。区块链可以将每一笔发生在数字账本上的交易都复制到其他用户那里去。这种“共享账本”的方法能够简化政府机关和经济运行中的很多服务。分布式账本是一种跨越多个站点、国家或机构的数据库，而且通常是公开的。数据是在一个连续的账本里按照先后顺序记录的，但并不是存储到区块里面。只有当参与者达成一定数量的赞成票后，记录才能添加到账本里面。

分布式账本需要信任账本的校验者或者是操作者。例如，全球性的金融交易系统瑞波（ Ripple）就使用了一组选定的验证者（被称为独特节点校验者），最多可以达到 200 个校验节点，它们是已知的、未知或者是部分信息公开的校验者，系统是基于它们不会合谋作弊的基础上运作的。这个过程提供了一个与比特币相比可能会有审查元素的数字签名，但速度要快很多。

区块链是一种数据库，它将记录存放到一个区块里。每一个区块是使用密码学签名与下一个区块“链接”起来的，这可以在任何有足够权限的人之间进行共享和协作。

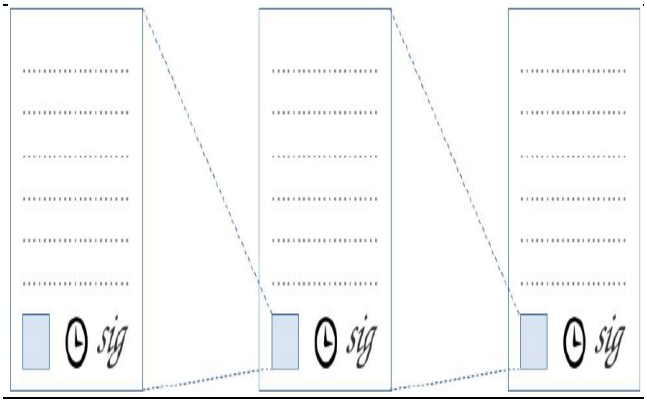
TCP/IP 保畅通,区块链保真实

TCP/IP 是互联网的基础协议，可以直白地理解成“计算机通讯协议”，这是互联网的基础协议。TCP 负责进出口（IO 总线）无缝对接，IP 负责通道畅通。TCP/IP 协议解决了信息传输的问题。

但是，TCP/IP 还没有解决信息被造假的问题，不能保证对方传过来的数据是真实的。区块链是互联网基础协议的升级版，该基础协议本质很简单，就是盖时间戳，全网一起记账、一起公证，而不是相信某一个人，这就实现去中心化的目的。

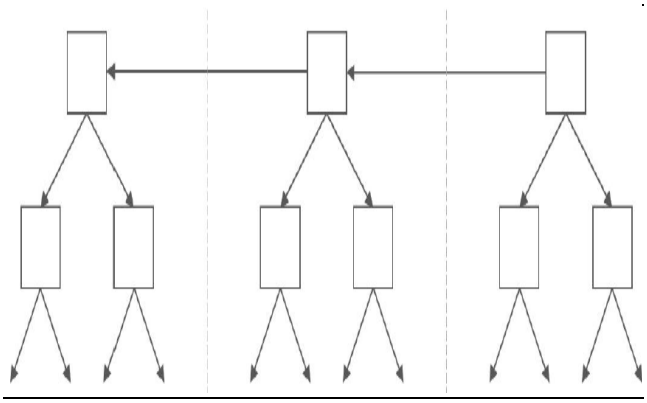
区块链技术背后的设想很有历史， 1991 年 Haber 和 Stornetta 设想用户可以将文件发送到一个时间戳装置那里盖时间戳（即时的）并生成一个附有相关信息的“证书”。这保证了文件的真实性，事实一旦发生，历史记录就无法被改变。

图 1： 串联的时间戳



资料来源：普林斯顿《比特币和加密货币技术》，国信证券经济研究所整理

图 2： 高效的时间戳链条



资料来源：普林斯顿《比特币和加密货币技术》，国信证券经济研究所整理

后来有作出效率上的改进：比起分别对文件建立联系，可以将他们打包在一起形成区块，并将区块连成链条。在每个区块中，文件之间依旧联系在一起，但是是以树状结构而不是线性结构。这样就不用为了确定一个特定的文件出现在系统中的特定的时间而实施那么多检查。这个混合模式正如图所示。

这个数据结构就构成了区块链技术的骨架，哈希协议被用来控制新区块加入链条的速度。这个修正对区块链的安全模型意义重大。再也不需要可以信任的服务器（中心服务器），取代它的是很多不可信的节点，每个接入网络的设备都可以成为节点，通过创造区块解决计算难题。依赖于哈希指针来保障数据结构的真实性，系统的关键点在于用一种防篡改的方式记录交易的顺序。

三步走理解区块链技术原理

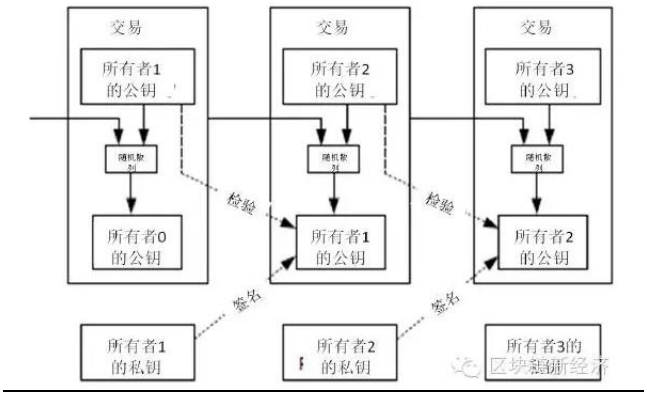
区块链网络通过随机散列对全部交易加上时间戳，将它们合并入一个不断延伸的基于随机散列的工作量证明的链条作为交易记录，除非重新完成全部的工作量证明，形成的交易记录将不可更改。通俗讲，区块链的技术原理分 3 步走：

1.把一段时间内的信息打包成一个区块（赋一随机序列）；

2.盖上时间戳（用随机序列生成一个哈希值）；

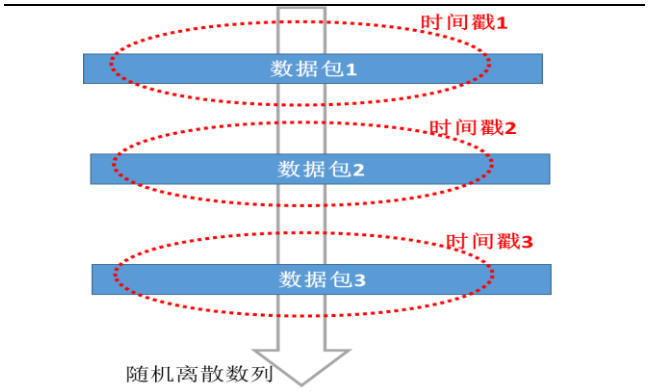
3.与上一个区块衔接在一起，形成新的区块。

图 3：专业解释图



资料来源：中本聪，国信证券经济研究所整理

图 4：通俗解释图



资料来源：国信证券经济研究所整理

每下一个区块的首页都包含了上一个区块的索引（专业名称哈希值），然后在页中写入新的信息，从而新城新的区块，首尾相连，最终形成了区块链。到 2016 年 3 月 18 日，比特币区块链上共有 403219 个区块，数据总容量 43GB，全网算力在 1000PFLOPS（每秒 1000 万亿次浮点计算），这些计算能力由全球接入比特币系统的无数台计算机免费提供的。目前我国的天河二号超级计算机的算力也只有 34 PFLOPS。

图 5：比特币领域的区块链数目

区块 / 最新生成的区块

区块高度	包含交易数	总发送额	数据量 (kB)	挖出方	生成时间
403219	1857	14515.83 BTC	976.41	鱼池F2Pool	2016-03-18 21:33:31
403218	2253	25540.15 BTC	976.44	鱼池F2Pool	2016-03-18 21:25:46
403217	2678	39964.82 BTC	912.50	AntPool	2016-03-18 21:14:32
403216	1603	8267.87 BTC	965.95	BTCC Pool	2016-03-18 20:52:14
403215	2489	48984.3 BTC	912.55	KnCMiner	2016-03-18 20:49:21
403214	1328	20173.93 BTC	974.76	BitFury	2016-03-18 20:30:02

资料来源： qukuai，国信证券经济研究所整理

密码是区块链的重要支撑

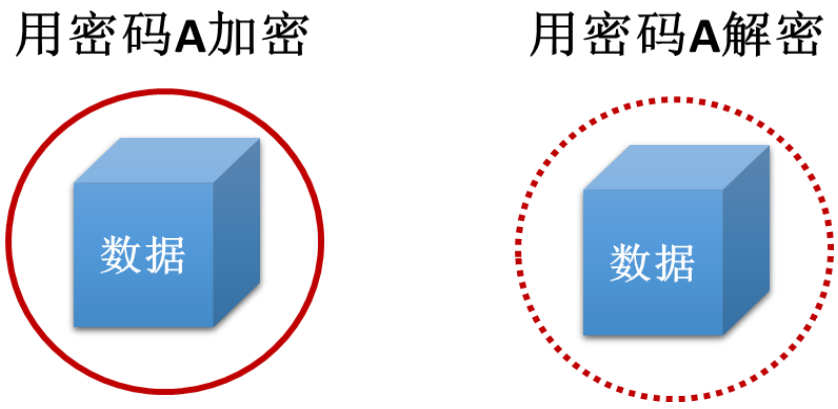
区块链算法让比特币的交易可以在“区块”里集中起来，并通过密码学签名添加到现有区块组成的“链”里面。比特币账本是用分布式及“无需许可”的方式构建的，任何人都可以通过解决生成新区块所需的密码学难题从而添加一个包含交易的区块。

这样区块链技术就实现了：一是用纯数学方法来建立各方的信任关系，二是交易各方信任关系的建立完全不需要借助第三方；三是建立信任关系的成本几乎降到零。

1976 年以前，所有的加密方法（例如摩斯密码、移位密码、字符替换等）都是同一种模式：

1.甲方选择一种加密规则，对信息加密；2.乙方使用同一种规则，对信息解密。

图 6：传统加密方式



资料来源：国信证券经济研究所整理

这种加密和解密使用的同一种密钥的对称加密算法有最大的弱点：甲方必须把加密规则告诉乙方，如此，密钥的传递和保存风险加大，尤其是公用密钥的人数增多之后。

1977 年，李维斯特、沙米尔、艾德曼设计一种非对称加密服算法——RSA 算法（三人名字组合）。RSA 加密模式流程：

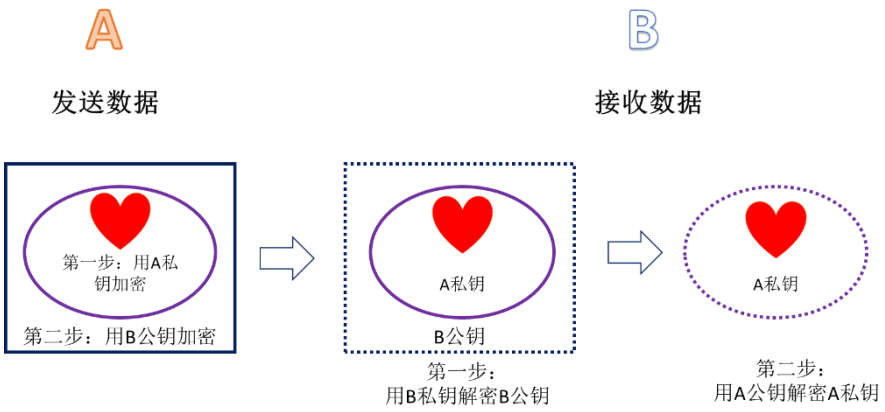
1.乙方生成两把密钥（公钥和私钥），公钥是公开的，任何人都可以获得，私钥是保密的。

2.甲方获得乙方的公钥，然后用它对信息加密。

3.乙方得到加密信息后，用私钥解密。

利用非对称加密算法信息发送流程既证明信息是 A 发出的，又能保证只有 B 才能解密。**私钥加密数据，用公钥能解密，但是用公钥加密信息只有私钥解得开，**因此只要私钥不泄露，通信过程就是安全的。

图 7：区块链的非对称加密方式



资料来源：国信证券经济研究所整理

A 发送信息到 B 的加密解码过程如下：

第一步，用 A 的私钥对原始信息做第一层加密；第二步，在上一步获得数据基础上再用 B 的公钥做第二层加密。第一层加密的目的是为了证明这个信息是由 A 加密并发出的，因为只有 A 的私钥才能完成这样的加密，这一步叫数字签名；第二层加密的目的是确保信息只有 B 才能解密，因为 B 的私钥只有 B 才有。

B 收到信息后，第一步，用 B 私钥对解密信息；第二步，在第一步获得的数据基础上用 A 的公钥再次解密。第一步顺利完成，可以确保只有 B 自己才能解密，其他人是无法解密的。第二步顺利完成，让 B 确保信息是由 A 的私钥加密发出的，排除了被别人伪造的可能。

在 RSA 基础上又衍生椭圆曲线算法（ECC），也是一种非对称加密算法，ECC 各方面的性能都比 RSA 更胜一筹：1.安全性更高，例如 160 位的 ECC 比 1024 位的 RSA 有相等的安全强度；2.计算量小，处理速度比 RSA 快得多；3 存储空间占用小，密钥尺寸和系统参数与 RSA 相比要小得多；4.带宽要求低。

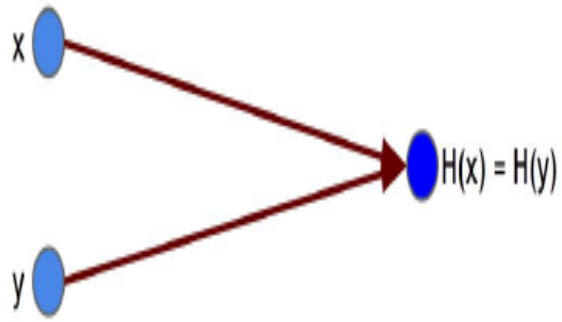
牵一发而动全身：密码学中的哈希函数保证了数据不能篡改

要知道为什么区块链分布记账不能篡改，要从密码学中的哈希函数说起。**密码学的哈希函数有三大性质：免碰撞、隐匿性、解谜友好，支持区块链成立。**

- **免碰撞性（Collision resistance）——**碰撞是指两个不同的输入映射出相同的输出。如果无法找到两个不相等的值 x 和 y 使得 H(x)= H(y) 的话，就说这个哈希函数 H 是免碰撞性的。

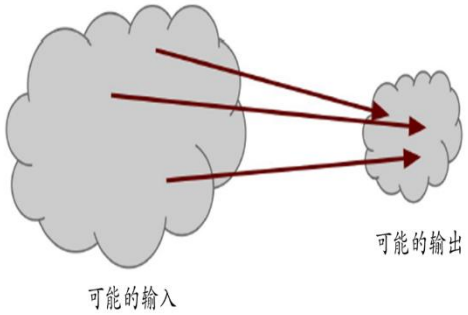
虽然没人可以找到一个碰撞，但并不意味着碰撞不存在。事实上，碰撞是存在的。输入空间包括任意长度的任意二进制串（无穷的），但是输出空间却只包含特定长度的二进制串（有限的）。输入空间大于输出空间，所以必定是有不同的输入映射出相同的输出。

图 8：哈希函数碰撞



资料来源：国信证券经济研究所整理

图 9：输入大于输出



资料来源：国信证券经济研究所整理

理论上碰撞是存在的，但是，问题是，普通人用日常的计算机不能找到碰撞输出结果。理论上在可能的输入中选取 2 的 130 次方个随机选择的输入，如果我们选择这些输入有 99.8%的概率，至少其中两个的输出结果是碰撞的。

但是，这个方法消耗的时间太长，将哈希函数运行 2 的 130 次方，而 2 的 130 次方是一个天文数字，换句话说如果人类有史以来制造的所有电脑从宇宙诞生一直计算到现在，他们找到一个碰撞的几率，依然是无穷小。因此我们知道如何找到一个碰撞，但是这个方法耗时太长.但这里我们就是说找到碰撞是不可能的。

免碰撞应用举例：我们有一个超级大的文件，想要在之后确认另一个超大的文件是不是我们原来看到的那个。一种方法是直接比较原文件的内容，但文件很大，比较很麻烦；另一种方法是记住原文件的哈希值，当有人宣称另一个文件与之相同时，我们可以计算新文件的哈希值，如果哈希值相同，我们就可以认为这两个文件是相同的。因为哈希值很小，只有 256 位，而原文件可能非常非常大，因此哈希是很有用的信息摘要工具。

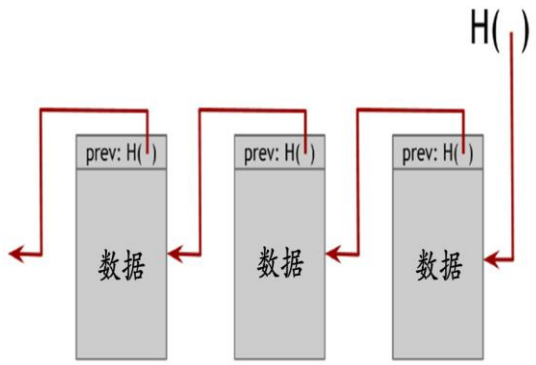
- **隐匿性（Hiding）：**如果已知哈希函数 y=H（x）的输出结果 y 从而想得到输入值 x，在计算上是不可行的。对一个给定的哈希函数的输出，没有可行的方式可以找到输入是什么。

- **解谜友好（Puzzle friendliness）**：对每个可能的 n 位大小的输出值 y，如果 k 是从有着较大最小熵的分布中选取的，那么无法在显著少于 2^n 的时间里找到 x 使得 H（k|x）=y。这个性质比之前的又更复杂了一些。对任何你想要从哈希函数得到的输出值 y，如果 k 来自一个高最小熵的超级广的分布，那么无法找到一个 x 使 H（k|x）=y。有些人想要锁定哈希函数的哈希值，他们想要哈希出一些特殊的哈希值 Y，而如果输入是合格的随机分布的话，是很难找到另一个值正好哈希值属于这个目标 Y 的。**通俗讲就是：求解哈希函数只能用穷举法一个一个去试，不能直接求解。**

使用哈希指针建立的串联列表，这种数据结构就是区块链。就像常规的串联列表，**每一个区块包含自身的数据和上一个块的指针**。在这里上一个块的指针替换为哈希指针，从哈希指针可以找出上一个区块的位置和内容。

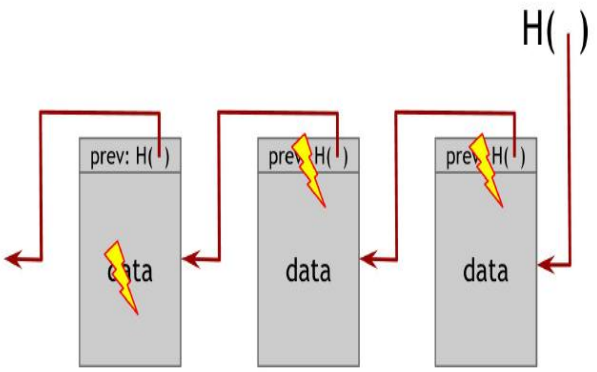
如果要建立一个日志数据结构，存储一堆数据，我们可以在日志的尾部增加数据。但是如果后面有人弄乱日志前面的数据，我们将能够发现这种行为，这就是防作弊。要理解为什么区块链具备这样的防作弊性质，让我们看看如果有捣乱者试图篡改链条中间的数据会发生什么。

图 10：区块链



资料来源：国信证券经济研究所整理

图 11：篡改数据图示



资料来源：国信证券经济研究所整理

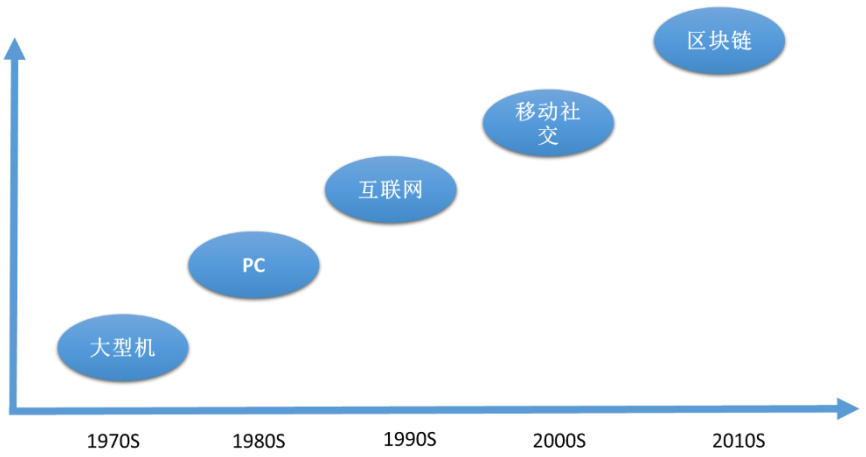
如果篡改左边区块的数据，由于哈希的免碰撞性质，会改变中间区块上方的哈希值。如果继续篡改中间区块的哈希值，造成的结果是又改动了中间区块的数据，中间区块的数据改变，由会导致右边区块哈希值，右边哈希值变化会引起右边区块数据变化，右边区块数据变化会导致原始的哈希值变化，而原始的哈希值是我们共有的。

因此结果是，如果篡改者想要改动整个链上任何一处的数据，为了不被发现，它将不得不一路修改哈希指针，他最终会无能为力，因为它不能改动表头。这意味着只要记住上面这个哈希指针，通过这种方法我们就记住了整条链。我们可以像这样构造随便多长的块链，在列表最开始的那个特殊的块我们可以称之为创世块。这就是一个通过块链构造的防作弊日志，也就是牵一发而动全身。

第五次颠覆性的新计算范式

分析现代社会进化过程的一种方法是观察计算范式，我们看到每隔 10 年就会有一次新的范式出现。首先是大型机和个人电脑范式，然后互联网革新了世间万物，移动手机和社交网络是最近的范式。接下来是 10 年，基于区块链加密协议的网络很有可能就是新的范式。

图 12：颠覆式计算范式演变



资料来源：国信证券经济研究所整理

这种新网络世界可以有效地利用区块链科技作为经济层，基于正日益形成一个包括可穿戴设备、物联网传感器、智能手机、平板电脑、量化的自我跟踪设备、智能家居、智能汽车和智慧城市等多种设备的无缝对接的世界。这种区块链能够实现的不仅是金钱的流动，它更是信息的转移和资源间有效的分配。

公开的分布式账本代替 VISA 清算

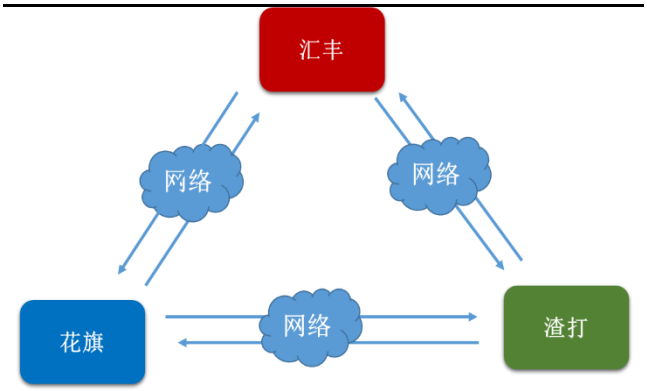
区块链的本质是一个公开的、分布式的账本，拥有成为所有资产的登记、编册、和转让的全球性的、去中心化的记录的潜力，这些资产不仅包括资金，也可以应用于股票、软件、健康数据和思想等各类财产和无形资产。

分布式账本，从实质上说就是一个可以在多个站点、 不同地理位置或者多个机构组成的网络里进行分享的资产数据库。在一个网络里的参与者可以获得一个唯一、真实账本的副账本里的任何改动都会在所有的副本中被反映出来，反应时间会在几分钟甚至是几秒内。在这个账本里存储的资产可以是金融、法律定义上的、实体的或是电子的资产。在这个账本里存储的资产的安全性和准确性是通过公私钥以及签名的使用去控制账本的访问权，从而实现密码学基础上的维护。根据网络中达成共识的规则，账本中的记录可以由一个、一些或者是所有参与者共同进行更新。

VISA 提升结算速度降低成本

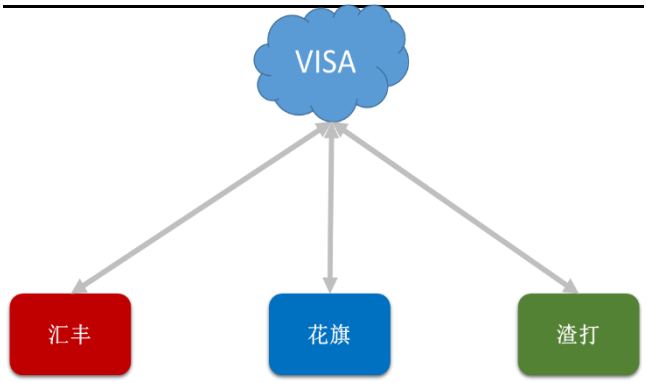
生活中我们经常需要跨行、异地存取款，这会给银行之间带来高昂的结算成本。在没有银行间清算组织之前，需要解决两家银行之间的通信、结算等问题。汇丰银行、花旗银行、渣打银行之间需要有专门的通信接口，满足双向通信的需求。

图 13：最初的跨行取款银行间财务关系



资料来源：国信证券经济研究所整理

图 14：有银行间组织的银行间结算



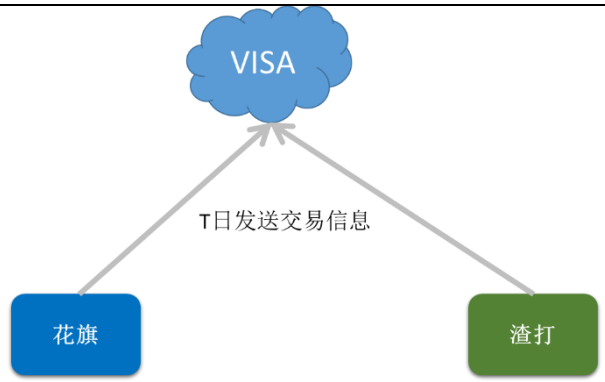
资料来源：国信证券经济研究所整理

在没有卡组织之前，同业银行之间的来往增多以后，会快速增加银行之间的清算速度和成本。当有三家银行的时候，通信链路就有 3*2=6 条，当银行越来越多的时候，这种点对点的通信变的越来越复杂，每新增一家银行，他要做之前银行都要做的很多重复性的劳动，这样的成本非常高，也不经济。如果一家银行与业内的 1000 家银行之间建立清算链接，该银行需要建设 1998 条通信路线。类似足球比赛中主客场之间比赛，20 支球队之间的联赛，每支球队需要参加 38 场比赛，30 支球队的联赛每支球队需要踢 58 场比赛。

那么必须出现一个网络，它能够接入所有的银行，新的银行只需要接入这个网络，就可以和其他所有的银行进行通信。

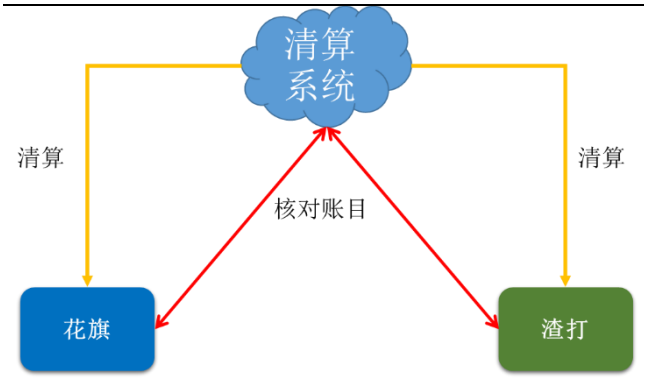
从技术上来讲，如果每一笔交易都要保证金实时记账，那么保证金系统的负载太大，事务如何保证等等一些列的问题。所以一般都是在 T 日之后清算。

图 15：清算系统 T 日发生跨行交易（通信系统）



资料来源：国信证券经济研究所整理

图 16：清算系统 T+1 日清算（清算系统）



资料来源：国信证券经济研究所整理

分布式结算成本降低至零

互联网上的贸易，几乎都需要借助金融机构作为可资信赖的 VISA 等第三方来处理电子支付信息。虽然这类系统在绝大多数情况下都运作良好，但是这类系统仍然内生性地受制于“基于信用的模式”的弱点。我们无法实现完全不可逆的交易，因为金融机构总是不可避免地会出面协调争端。

通过上一节中的 VISA 案例，我们看到金融中介的存在，也会增加交易的成本，并且限制了实际可行的最小交易规模，也限制了日常的小额支付交易。

并且潜在的损失还在于，很多商品和服务本身是无法退货的，如果缺乏不可逆的支付手段，互联网的贸易就大大受限。因为有潜在的退款的可能，就需要交易双方拥有信任。而商家也必须提防自己的客户，因此会向客户索取完全不必要的个人信息。而实际的商业行为中，一定比例的欺诈性客户也被认为是不可避免的，相关损失视作销售费用处理。而在使用物理现金的情况下，这些销售费用和支付问题上的不确定性却是可以避免的，因为此时没有第三方信用中介的存在。

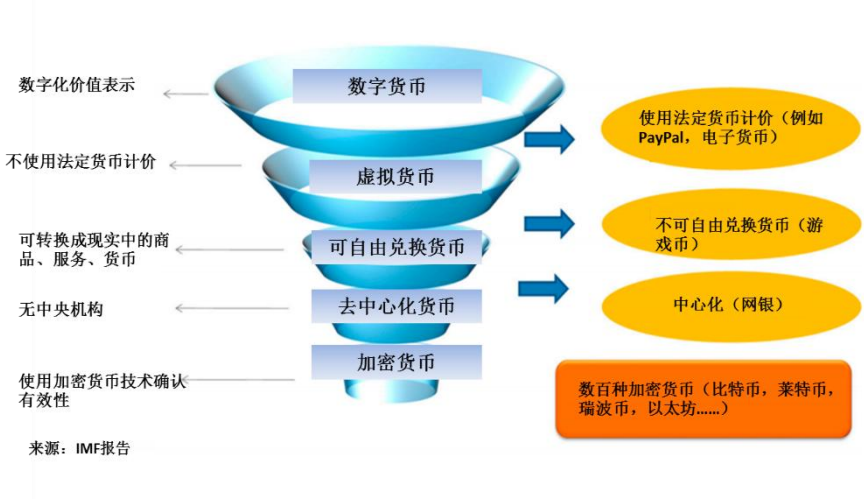
所以，我们非常需要这样一种电子支付系统，它基于密码学原理而不基于信用，使得任何达成一致的双方，能够直接进行支付，从而不需要第三方中介的参与。

比特币发起人中本聪提出通过区块链的点对点分布式的时间戳服务器来生成依照时间前后排列并加以记录的电子交易证明，从而解决双重支付问题。只要诚实的节点所控制的计算能力的总和，大于有合作关系的攻击者的计算能力的总和，该系统就是安全的。

记账新工具：虚拟货币

随着价值数字化表示，虚拟货币可纳入更广泛的数字货币种类中。但是它们与一些数字货币又不同，例如电子货币（法定货币计价的电子支付手段），但是虚拟货币不以法定货币计价，它们有自己的记账单位。

图 17：虚拟货币分类



资料来源：IMF，国信证券经济研究所整理

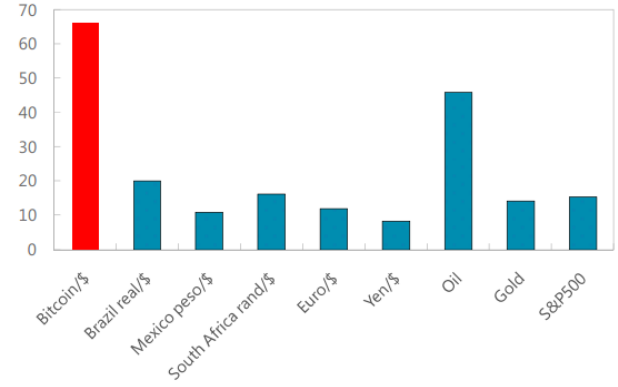
虚拟货币价格的高波动性限制了它们价值贮藏的能力。国家和企业不使用虚拟货币计量债务，因为其价格十分不稳定，波动性十分显著地超过了一些货币对，且价格和波动性与与经济金融因素无关，不易于做套期保值或预测。

过去的几年里，比特币价值波动性十分大，超过任何主要货币和资产。

图 18：比特币价值(美元/每单位比特币)

资料来源：OKCOIN，国信证券经济研究所整理

图 19：2015 年比特币和部分货币/资产的波动性



资料来源：BTCC，国信证券经济研究所整理
注：每日价格变化的标准差，以年化百分比表示。

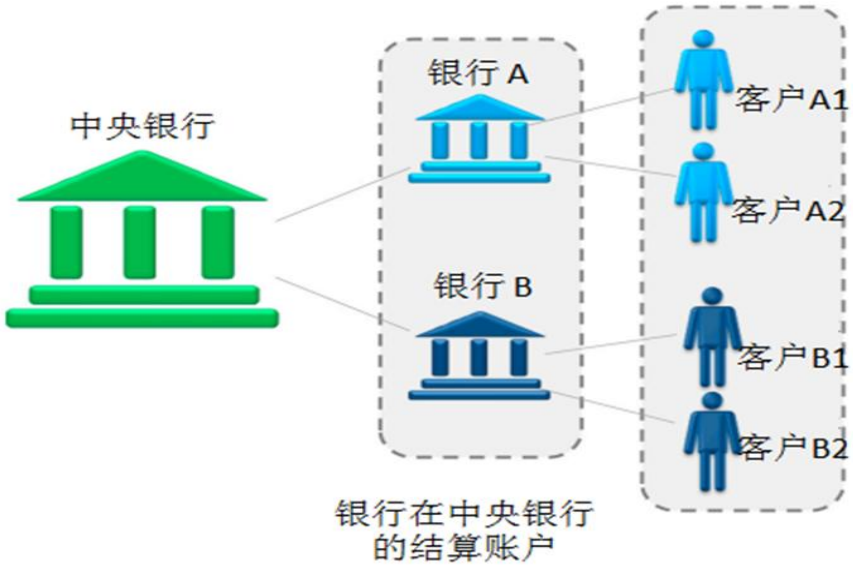
记账新方式：央行集中式记账到分布式记账

交易时需要记账，现代支付系统通常是中心化的。中央银行在中央分类账的账户间划拨款项，处理成员金融机构的清算、结算请求，成员金融机构再在内部分类账间调整客户账户头寸。

中央银行负责在中央分类账中精准、即时地确认交易，防止重复支付或造假。

整个系统的稳定性依赖对执行信用中介功能中央银行的信任 ，和央行维护中央分类账正确性的能力。

图 20：银行在中央银行的结算账户



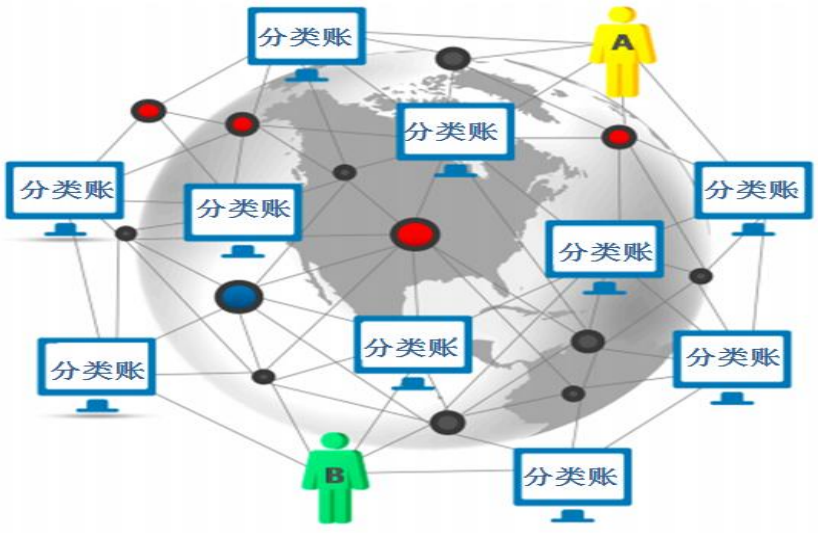
资料来源：国信证券经济研究所整理

客户 A1 向 B1 支付过程:

1) 款项从 A1 在银行 A 的账户里划出
2) 央行将款项从银行 A 的结算账户划至 B 的结算账户中
3) 央行确认交易，防止重复支付和造假，保留银行间交易的核心记录（分类账）
4) 银行 B 把款项划至 B1 账户

5） 银行 A、B 分别记录客户 A1、B1 的交易分类账

图 21：分布式记账系统



资料来源：IMF，国信证券经济研究所整理

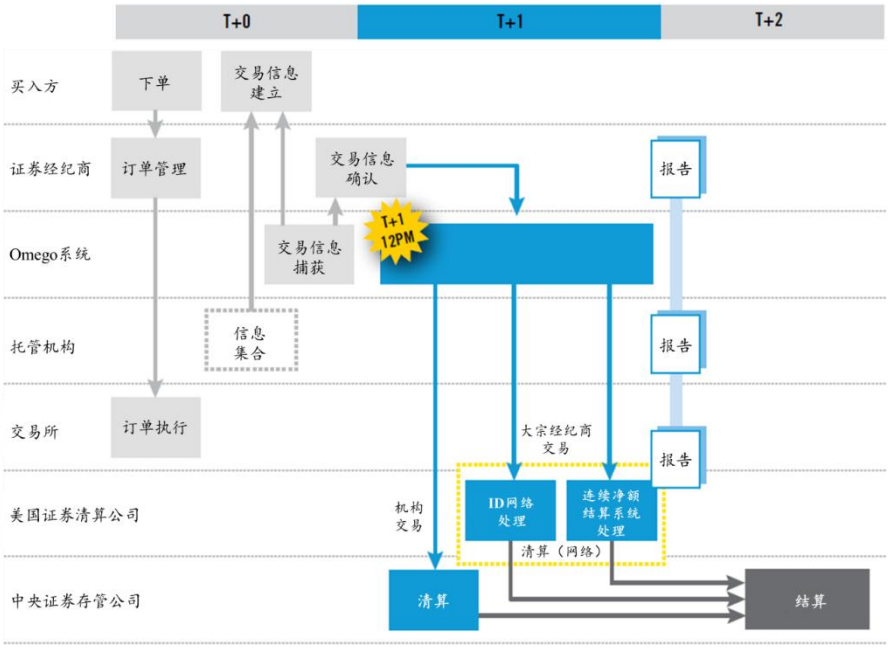
分布式账本技术代表一种朝着激进方向的创新，因为它有潜力影响到大范围的商业模式：从新的产品到服务，通过操作系统和组织结构，并且还有许多潜在的行业可能会被影响。因此，他们会互相关联，并且和内部关联突破，形成一次技术革命。

清算组织从无到有再到无

清算、结算、托管和注册服务，对于发行、交易和持有证券都会增加显著的成本。有大量的专业代理和交易对手参与到投资者的证券和现金活动中。不仅这些服务有特定的收费， 也有相关处理各种不同系统接口的业务集成和流程的辅助成本。总体而言，全球金融行业每年在交易后“post-trade” 成本大约是 650-800 亿美元。

现在主流证券交易结算是多层次的复杂交易过程，下图解释了目前市场上实施的 T+2 交易机制。

图 22：美国证券交易托管结算体系



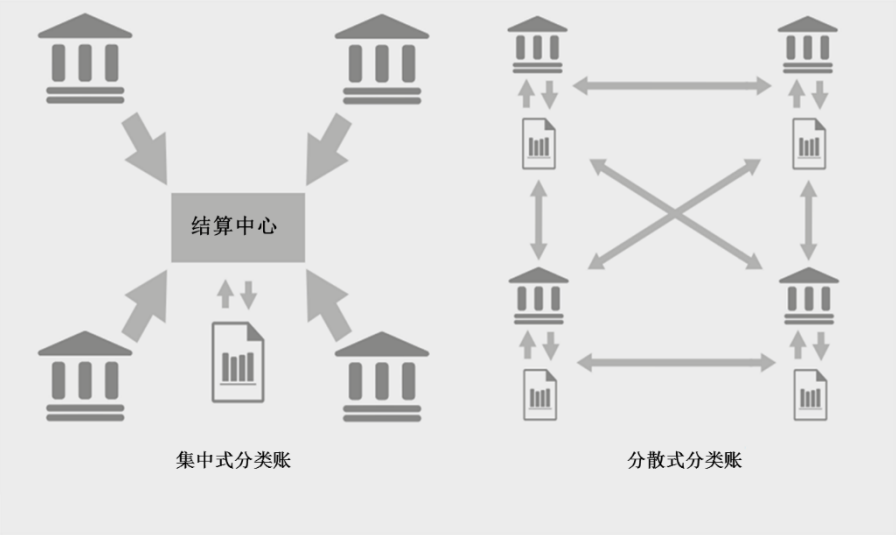
资料来源：《DTCC：拥抱分布式》，国信证券经济研究所整理

区块链技术提供了一个显著降低这些复杂性和交易后的服务成本，参与者来操作存在于大量作为节点来运行的服务器上存储的共享式账本。而执行交易的权利是由密码学设置的公私钥来决定的。

交易能够被添加到数据库中的块，每一个区块都会由节点进行审查。如果所有节点达成共识，认为该区块包含有效交易时就会被添加到数据库中。此外建立和维护这些节点，这个区块链网络应该是完全自治的，不允许任何一个控制或者监管实体存在。

区块链清算是技术，分散式记账是表现形式。分散式分类账是一种通过共享注册表记录所有权的网络结构。相比于现在的交易网络，分散式分类账取消了清算中心。可以开放核实匿名者，也可以关闭只供识别用户接入。最著名的应用是加密货币比特币。

图 23：集中式和分散式分类账比较



资料来源：桑坦德银行报告，国信证券经济研究所整理

分散式分类账的优点：

交易不可取消，清算和结算几乎达到同步；系统在对等网络上运行，交易能确保正确执行。每笔交易都能被网络社区的用户核实，而不是只靠一个中心机构，因此交易会更难被篡改。几乎所有无形的文件或资产都能被编程以代码的形式表达。交易历史可以被记录且公开，使得监管者、参与者能更有效地监管。

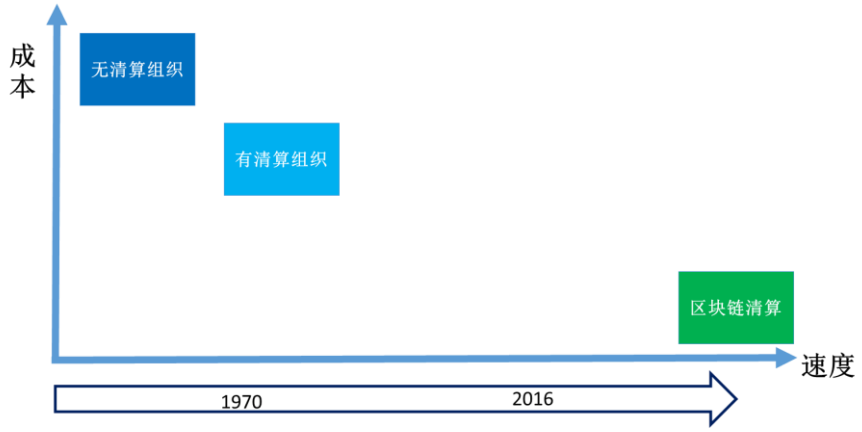
图 24：分布式总账技术特征

标准化	分布式总账技术的运用是否有助于产业在数据格式和契约规则方面的标准化？
效率	分布式总账技术和其它系统之间是否可以消除人工交互，解决数据交换、数据格式转换和一致性的问题？
更快进程	分布式总账技术是否可以为完成一项交易节约时间并降低风险？
透明性	分布式总账技术带来的透明性是否对其技术的商业化运用产生效益？
安全性	分布式总账技术自带的授权和加密是否提高了业务流程及其数据的整体安全系数？

资料来源：DTCC，国信证券经济研究所整理

在 VISA、万事达等这样的卡组织出现之前，跨行结算复杂度很高，成本高、速度超级慢。卡组织出现后，形成中心清算的模式，所有银行和该中心建立清算接口，所有跨行之间的交易都汇总到该清算中心。也就是清算组织的出现提升了了跨行清算的速度，并降低了清算的成本。

图 25：清算组织从无到有



资料来源：国信证券经济研究所整理

由于是中心集合模式，随着加入组织的银行成员增多，给清算中心带来收入的同时，也加大了工作量。在接入的银行超过一定程度后，在增加银行会员，就会显著增加清算中心成本和工作量，从而降低清算速度。例如管理 10 人团队和管理 10000 人团队差别很大。

在目前国际上有六大信用卡品牌，分别是 VISA、万事达、美国运通、中国银联、大来、JCB 日本国际。VISA、万事达、美国运通三家上市公司 2015 年营业收入合计 543 亿美元，区块链技术实现分布式记账的结算之后，能为整个银行业节省一大笔费用。

分布式记账案例

（以下案例来 A report by the UK Government Chief Scientific Adviser）

分布式账本技术对于操作成本上有巨大的好处。 它们不仅内部成本很低，还能够避免重复和无效率的管理和协作，通过一个通用、公开、能够完成工业级的操作，就像通过在每个个人持有的账本和数据库进行交叉检查，这样可以降低因为流程造成的成本。它可以数字化和安全的存储任何资产的信息，从钻石到几袋大米，能让企业标识并跟踪他们的所有权和位置（钻石认证案例）。

通过使用分布式账本技术，通过开发可编程的智能合约来进行记录和传递价值：例如以太坊（ Ethereum），是一种称为“智能合约（ SmartContracts）”的去中心化平台。他们具有颠覆性的潜力可能会扩展到任何一个新的场景，只要存在具有信任或者被垄断经营的中介——一个“ 中心辐射” 模式——都会被涉及，或者被更开放的模式取代，基于更加扁平社区的共识结构（公司行为案例）。

分布式账本技术的开发和相关联的技术提供实时记录交易的可能性，使得交易更加快捷、成本更低。例如，汽车保险可以基于汽车和它驾驶者的情况，保险可以根据行为、价格和风险偏好来进行动态改变。（SETL 案例）

由此将会诞生“ 可编程经济” ，通过智能合约，依靠去中心化的网络和机构，只需要很少的人参与，作为一种分布式自治组织来大范围提供产品和服务。

钻石案例：

钻石行业是一个很容易出现犯罪活动的行业。钻石体积很小，而且能够以隐藏的方式来传输，交易可以被保密，而且钻石在很长的时间内都是保值的。因此，钻石经常被卷入到全球范围的洗钱或者恐怖主义融资行为中。

为了遏制这种非法活动，包括通过纸质文件来追踪钻石和确认它们的来源。但是，文件篡改是非常普遍的行为——事实上，文件经常用于创建来掩盖非法交易的—目前几个主要进行钻石交易的国家，仍旧没有足够的法律来防止这些犯罪。

为了解决这个问题，钻石行业开始实施一个名为 Everledger，基于区块链技术的系统，它能够为每一颗钻石建立一个数字“护照”。能够记录来源、经历，和通过一个唯一的数字加密“指纹”进行交易。

这个系统有三个阶段:

1. 为每一个钻石建立一个 e-ID（电子身份），通过数字化它的属性，将激光刻下的序列号放置在一个可以认证的区块链账本上。
2. 为钻石指定一个数字护照来记录它的履历，交易历史和起源。
3. 检测和防范非法活动或者欺诈行为。

通过使用不可更改的区块链来保存数据，分布式账本可以完全透明的提供所有钻石、揭示它们的来源，跟踪它们的所有权，以及它们可能经历的过程。这种账本可以作为钻石行业、政府、 消费者市场、边境管制和执法力量的一个单独可以验证的强大工具。这个系统也能够使用智能合约——能够将钻石销售和传输的条款和条件相关联，就能自动开始执行。通过使用区块链来建立一个分布式账本，智能合约可以用于追踪，验证业务关系和协议。区块链的透明度能确保合同得以执行，根据钻石所有权，钻石的融资情况，保险条款，注册权等等。通过真实性证明文件的认证交易，将会为政府和支付机构提供重要的证据线索。

公司财报案例:

上市企业必须要以结构化格式来提供他们的年度账目。超过 90%的公司行为是由数据供应商来发布的，信息是从来源人工提取的、解释和重新录入的。不仅自动化水平很低，而且错误频繁，处理效率非常低下。预计公司财报处理成本每年大约高达 100 亿美元。

区块链技术能够让整个过程变得更有效率。公司行为代表了合同化信息和价值，原则上能够直接自动在收付款人之间进行传输，而不需要有中介参与，为各方提供可以信任的数据源，并且具有必要的经验来处理收到的信息。

如果区块链能够连接一个应用，用于捕获和存储结构化格式的企业行为公告，它就能够用于确保该数据是来自一个可以验证的来源，并且验证它发布时候的时间戳。这也可以被用于反向执行来完成。一个基于区块链技术的分布式账本，能够让参与的各方来确保信息的是精确、及时的，而且从发布者到他们手上都是未经篡改过的。

从理论上讲，它可以消除发布者和基金经理之间的所有中介机构，保证信息的准确性和及时性。这些中介机构可能会在信息通过他们前修改或者变更数据，经常会出现原始公司行为已经被改变，通过后续发布公告将会要求取代较早时间发布的公告。当数据提供商和他们客户进行分享，或者将其数据进行打包，这些修改的数据能够快速失去其来源，让整个过程难以自动化执行。

就其本身而言，区块链技术目前在处理不断变化的数据包时，速度还是比较缓慢。比特币区块链每小时只能处理 2 万笔交易，必须要长达一个小时的时间才能信任一笔交易，这对于公司财报研究是非常不方便的。也就是说现阶段用区块链技术进行

公司研究，可能需要更长的时间去等待验证。

位于 Monmouth 的公司 Codel，正在处理公司行为数据，其提供的基于区块链系统的数字认证软件，已经克服了这些问题。这个系统将创建一个不可更改的审计追踪，让链上的各方能够参考，来鉴定其真伪，提供有关数据来源的有价值保证。

他们在行业参与者和 Codel 之间有一个协作企业，一个可以搜索的企业行动信息并且登记在注册表中。这个注册表数据是以 ISO 15022 和 ISO 20022 格式进行存储，并且对金融信息提供提取的规范，能够转变为机器可以读取的格式，这意味着注册表能够根据公司行为对信息进行修改或者替代，实时进行更新。这保证了信息的完整性和精确性，通过 SWIFT 安全网络，能够让参与公司行为链的各方都可以使用。这克服了单独使用区块链造成的验证延迟，和信息——作为分布式账本有效分享——能够被更新、发布和实时修正，确保是正确和最新的。

政府可以通过改变规则，要求企业来发布企业行为信息时启用分布式账本接，来让该系统获得进行更好的发展。

SETLing 交易案例:

一个名为 SETL 私人投资企业打算开发和部署一个专用的区块链，能够让金融市场参与者在一个点对点基础上来结算证券交易，并且维护一个分布式证券“ 金” 账本和现金余额。特别是， SETL 目标是让央行能够在区块链上发行货币。它的区块链运行在一个自治基础上，能够和现有金融市场、支付和交易所基础设施进行整合，STEL 将能够同时处理证券和现金端的每一笔交易，允许单边传输证券和现金，无论简单的支付，还是结算定制合同、公司行为、股息和优惠券。

SETL 设计的目标是，将成本昂贵、具有风险的清算结算流程，变成一个对手方之间实时结算流程，此外，通过建立一个所有权的金账本， SETL 能够大大降低证券登记托管的开销。

STEL 区块链将有以下的特征:

- SETL 区块链中公钥将需要由认证机构发布，能非常清楚的确认拥有每一把认证私钥的区块链使用者。认证机构将会保留每个公钥使用者在现实世界的详细信息，符合反洗钱和 KYC 规则的要求。STEL 表示，如果有司法上的要求，认证机构将会透露这些信息。
- 将能够处理多种资产类别，包括现金和各种有价证券。
- 它将会使用多重签名交易，按照用户指定的用户群来完成授权。
- 将会使用“ 原子交易” （即所有的交易一旦发生，要么完成要么未完成），
- 这样，只有所有阶段被提交和被认证过，那么交易才能够处理。
- 它将包含一个特别的功能，特别为参与者管理流动性而设计。
- 出于简化监管记录保管、交易报告和审计的目的，它将会保留交易的完整记录和余额历史。

现金余额和其他资产倾向于保管在特定的系统，仅仅处于特定的目的而部署：换句话说，他们是“ 系统特殊部分” 。现金和资产放在一个区块链上，相反，能够由于任何目的来进行部署。这将会减少量，这样银行不得不部署流动性储备，并简化其流动性管理。STEL 系统能够提供一个解决方案，将会同时和现有的英国央行实时总结算系统（ RTGS， Real Time Gross Settlement）一起运行，在 RTGS 不可用的时候提供一个安全和可靠的选择。 RTGS 有些时间段是不工作，例如在晚上和周末的时候， SETL 将会是在任何时候都是可以工作的，减少的中间银行累积的风险。

SETL 支付和结算系统是简单的，统一和直接的。如果英国是第一个部署类似系统的，它将让伦敦和英镑成为金融服务行业未来的首选位置和货币。伦敦可能是全球首个建立类似系统的城市，系统可能越来越被广泛采用，将会进一步巩固伦敦的地位，成为国际金融的全球领导者。

全球金融的基础架构

未来建立信用的主要方式

未来全球市场信用是靠每个人自己参与公证和交易街垒起来的，区块链在商业和信息用的层面上，就是帮助建立该系统。把大数据变成分布式记账，参与记账的人越多，个人信用就越可靠。当区块链在更多的金融机构、商业领域使用的时候，吸纳更多的个人用户进来，用这个方式沉淀信息和个人信用。区块链最终的价值是信用积累的价值。

一个钢筋水泥为标志的银行信用大厦，正在被一个数据为土壤的区块链信用所取代。区块链就是靠全网分布记账，自由公证，建立了一个共识数据库，这就是未来信用的数据大厦。一个新的时代、未来的新信用是靠全网公证无数个计算机执行基础协议实现的。

非货币领域广泛应用

区块链技术的去中心化交易账本功能可以被用来注册、确认和转移不同类型的资产及合约。特别是第三方托管交易、债券合约、第三方仲裁以及多签名交易。

图 26：超越货币的区块链应用

分类	实例
一般	托管交易、保税合同、第三方仲裁、多方前面交易
金融交易	股票、股权、集资、债券、基金、衍生工具、年金
公共记录	土地和产权证、车辆登记、营业执照、结婚证
证件	驾驶证、身份证、护照、选民登记
私人记录	借据、贷款合同、投注、签名、中介
证明	保险证明、权属证明、公证文件
实物资产	家宅、酒店客房、汽车租赁
无形资产	专利、商标、版权、域名

资料来源：国信证券经济研究所整理

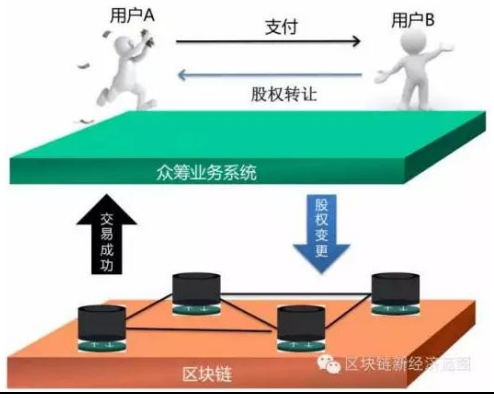
公共记录也同样能够迁移到区块链上，通过安全编码的形式来确认各种信息和身份。无形资产，例如为了保护某一个想法，不通过申请专利或者上边注册这些传统方法，而是将他编码放到区块链上，此时就能够获得一个有着某特定日期时间戳的证明，作为未来可以使用的证据。

区块链行业中主要的一部分就是利用数字货币来与传统银行和金融市场对接。美国旧金山的数字支付公司 Ripple 正在使用区块链技术来重塑银行业生态系统，让传统金融机构更有效地开展自己懂业务。Ripple 的支付网络可以让多国的银行直接进行转账和外汇交易，而不需要第三方中介。

案例：股权众筹

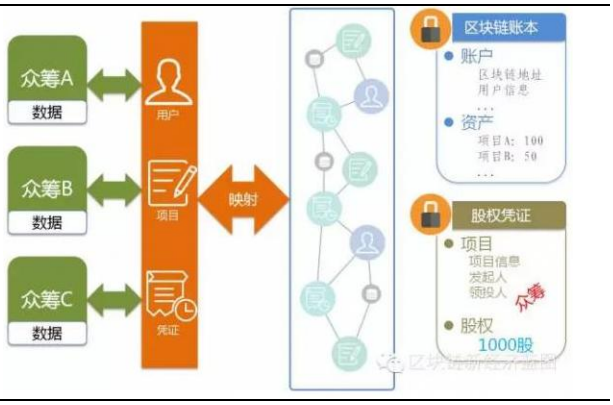
现有非上市股权管理，通常情况下，需要通过人工处理纸质股权凭证、期权发放和可换票据。如果出现频繁的股权变更，股东名册的维护将变得繁琐，历史交易的维护和跟踪也变得困难。区块链技术将会对这一切进行数字化管理，使其变得更加高效和安全。区块链众筹股权登记，将充分利用区块链账本的安全透明、不可篡改、易于跟踪等特点，记录公司股权及其变更历史。

图 27：区块链股权转让



资料来源：区块链新经济蓝图，国信证券经济研究所整理

图 28：众筹平台之间数据共享



资料来源：区块链新经济蓝图，国信证券经济研究所整理

对于股权众筹而言，股权流通是业务的重要一环，能够激发用户的活跃度，促使更多的登记发行。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。

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。

联盟最大的危机来自信任，由区块链构建的去中心化信任，天然适合联盟与协作。区块链技术构建的信任，不以人的意志为转移，在彼此不需要相互信任的前提下，也能保障系统和业务正常运行。每个众筹平台都成为区块链中的一个节点，拥有各自的公钥和私钥，共同参与交易验证和记账；另外除了众筹平台，监管机构也可以成为其中的一个节点，使监管变的更加透明、便捷。

要形成一个股权众筹联盟，首先要将用户、项目、以及所有权进行共享。如果按照传统的系统搭建方式，每个平台拥有独立的数据库，共享将变得异常复杂。如图 2 所示，区块链技术构建信任基础，能实现高效的数据共享。各个平台将自己的用户、众筹项目、股权凭证等映射到区块链网络中。

能够降低熵，创造一种新的网络组织

物理学角度看社会发展必须降低熵

注：熵是一个系统中"无秩序"的程度，也表征生命活动过程质量的一种度量。

区块链的潜在优势不仅局限在经济领域，还可以拓展到政治、公益、社交和科学领域。我们先从物理学入手，分析区块链在分布式社会中的作用。

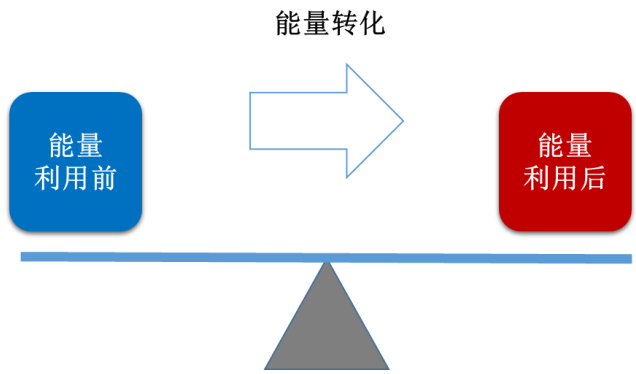
热力学第一定律：能量是守恒的，不会消失可以互相转化（电能转化为动能）。

热力学第二定律：不可能把热从低温物体传到高温物体而不产生其他影响，或不可能从单一热源取热使之完全转换为有用的功而不产生其他影响，或不可逆热力过程

中熵的微增量总是大于零。又称“熵增定律”，**表明了在自然过程中，一个孤立系统的总混乱度（即“熵”）不会减小**。

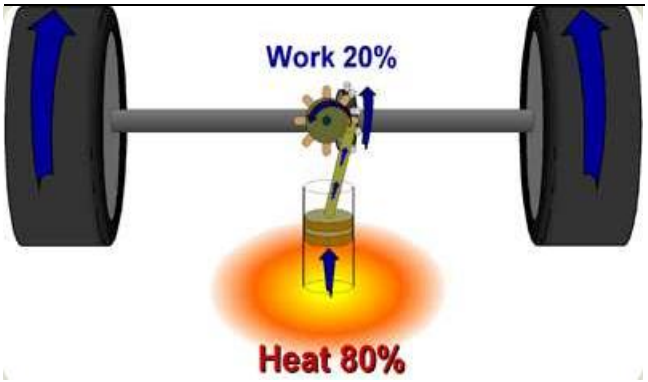
通俗解释就是虽然能量可以转化，但是无法 100%利用。在转化过程中，总是有一部分能量会被浪费掉。比如，汽油含有的能量可以转化成发动机的能量，但是会伴随产生大量的热能和废气。即使科技再发达，也无法将被浪费的能量减小至零。

图 29：热力学第一定律图示



资料来源：国信证券经济研究所整理

图 30：热力学第二定律图示



资料来源：国信证券经济研究所整理

用公式表达就是：能量的总和 = 有效能量 + 无效能量（用熵度量）。“有效能量”指的是，可以被利用的能量；“无效能量”指的是，无法再利用的能量，又称为熵。所以，熵就是系统中的无效能量。

考虑到宇宙的能量总和是一个常量，而每一次能量转化，必然有一部分“有效能量”变成“无效能量”（熵），因此不难推论，有效能量越来越少，无效能量越来越多。直到有一天，所有的有效能量都变成无效能量，那时将不再有任何能量转化，这就叫宇宙的“热寂”（Heat Death）。

所以，热力学第二定律的一个重要推论就是：熵永远在增加。

图 31：社会发展促使熵增加

资料来源：国信证券经济研究所整理

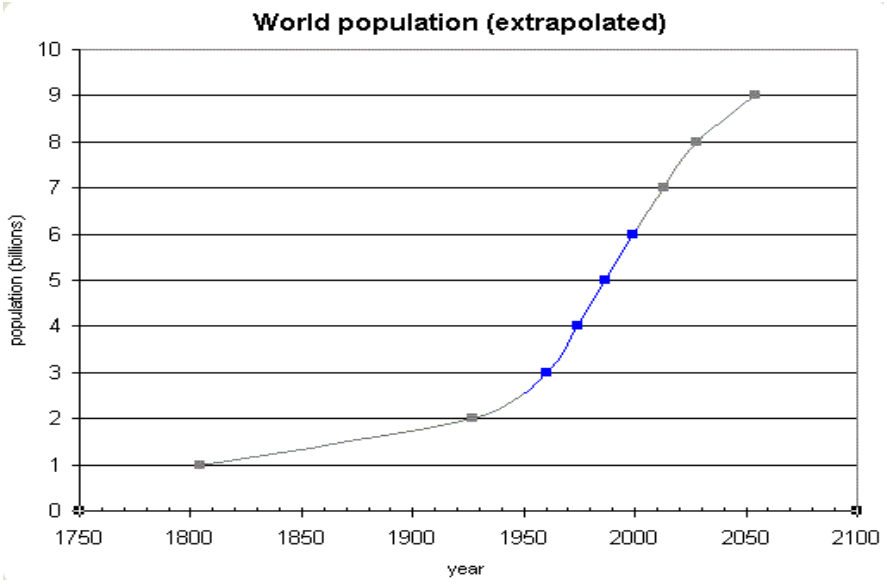
世界人口从 1804 年的 10 亿增长到 2014 年的 72 亿人，世界银行预计到 2025 年达到 80 亿，2045 年达到 90 亿。

世界人口在增长，以及由于生活水平的提高和维持现行秩序的需要，人类社会对能量的需求激增。如果人口增加 1 倍，所需要增加的能量将不止 1 倍。因此，能源的增长速度必须高于人口增长速度+经济增长速度，才可能支持人类社会现在这种发展。

比较能肯定的是能源几乎肯定无法这么快地增长。太阳能，以目前的技术，大规模

使用还不现实；化石能源，应该都会在本世纪内开采光；核能、水能和风能，将是未来的主要能源，但是都有各自的弊端（核废料、水坝、高昂的设备成本等等）。

图 32：世界人口增长趋势



资料来源：世界银行，国信证券经济研究所整理

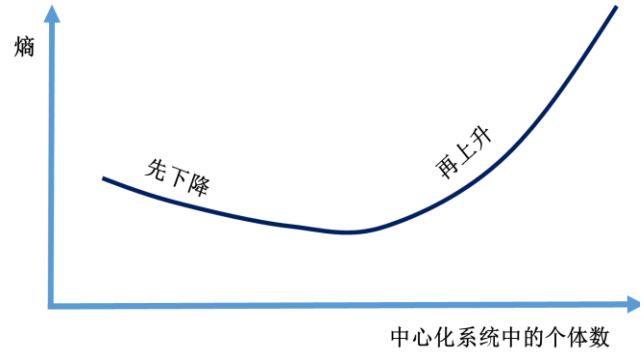
根据热力学第二定律，使用系统内的能源，必然增加系统内的熵。这意味着，如果人类单纯依靠地球自身的能源，地球必将变成一个越来越混乱的地方。

所以从熵的角度看，如果不改变发展模式来降低熵的增加，人类无法继续发展。区块链提供了另外一种发展模式。

蜜蜂筑巢式分布式管理增加有序降低熵

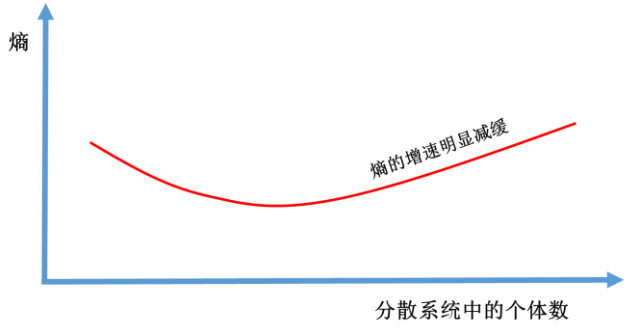
从信息学角度看，越中心化，系统的熵越容易增大。传统的方法都是把资源和信用想一个中心堆集，刚开始的时候，中心化系统中的个体数越堆集信用越大，但是随着系统中的个体数增多，熵开始升高。其实从物理角度看，堆集在一起后只能导致熵越来越大。

图 33：集中式、中心化的系统熵变化



资料来源：国信证券经济研究所整理

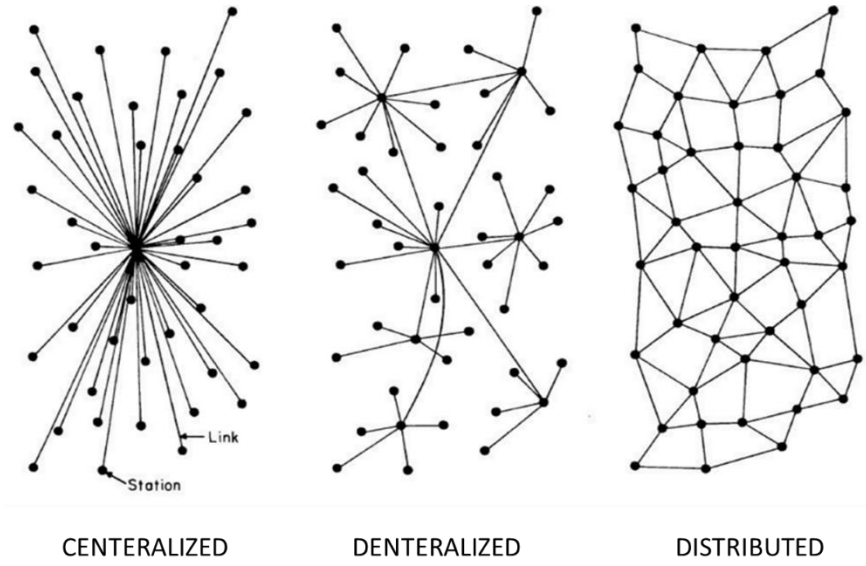
图 34：去中心化的社会熵增速放缓



资料来源：国信证券经济研究所整理

真正要想让一个系统的熵越来越小，信息和价值不断增大，就要走向分散化，同时每个点都执行基础协议。就像蜜蜂一样，每个蜜蜂智能执行很简单的基础协议，但是众多蜜蜂一起制造出来的蜂巢要比熊窝好很多倍，虽然单个的熊看起来又比单个蜜蜂有智能。

图 35：数字化社会结构图



资料来源：Blockchain，国信证券经济研究所整理

图中最左边的集中式系统的熵是不断增大的，因为只靠一个中心智能去产生信息不足以抵消整个系统的熵增加。

图中中间的去中心化系统会减缓熵增大的速度。

图中最右边的分布式系统才能让熵增速大幅减缓，因为系统中的个体都在发挥职能去产生信息，就像蜜蜂筑巢一样。

所以，要降低熵，只能分散化，每个顾客的作用只有一点点力量，但是群集分散就有群体智慧。例如淘宝等 B2C 平台，随着时间的推移，越来越多的小卖家加入，就会超过几年前 B2B 模式的京东（京东现在开始大力发展 B2C）。每个单独的小卖家再弱小，只要执行淘宝制定的基础协议，就能起到类似小蜜蜂一样的作用。如果将来区块链成熟应用后，保证每个商家在上面累积自己的信用，共同公证共享信用资源。

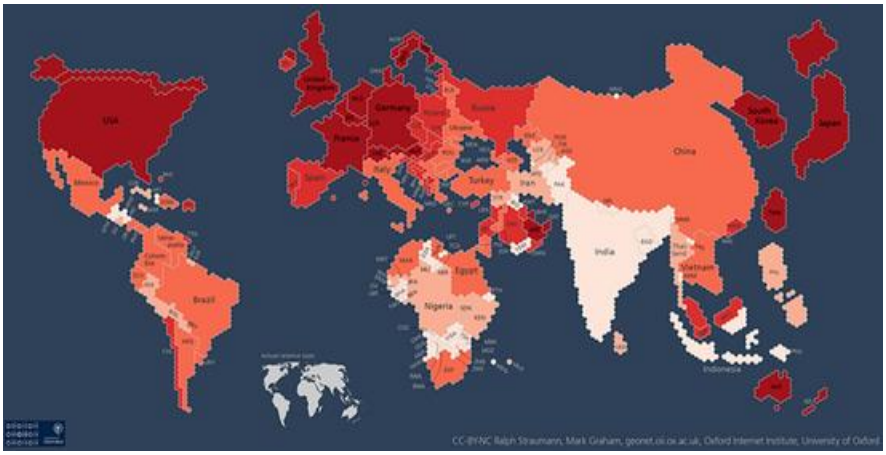
这个力量会强大到没有任何中心能够抵挡，而且保证阿里的整个系统的熵能够不断下降，这才能保企业长青。蜜蜂筑巢是人类佩服不已的一种建筑结构，耗费资源少、于环境融洽，也最符合蜜蜂群居的组织需求，这就叫群集智慧。

这就是从区块链延伸出来的人类治理模式，分布的点越多越能降低熵增加的速度。中国拥有世界第一多的互联网用户，为这种潜在的群集智慧提供了可能。

2015 年，牛津大学互联网研究所根据互联网用户人数制作了一张世界地图：每块区域都由小六边形组成，每块六边形代表 47 万互联网用户。在地图上，中国大陆面积最大，互联网用户数量居世界第一。

在地图上，因为各国网民人数相差很大，各国的领土形状和面积也随之改变了，有些用户数少于 47 万的国家在地图上消失了。具体来说，英国和日本的面积超过澳大利亚，俄罗斯则缩小到和法国、德国一般大小，中国成了“世界第一大国”。

图 36：互联网人口分布



资料来源：牛津大学互联网研究所，国信证券经济研究所整理

除了“领土”大小显示在线用户人数，“领土”颜色则显示当前该国在线人数占全国人口的百分比。深红色表示使用互联网人数占全国人口的 80%-100%，白色表示使用互联网人数占全国人口的 0-20%。在大小和人口百分比的对照上，印度显得格外突出：“领土”相对较大表示印度有很多互联网用户，“领土”为白色则表示印度互联网用户占其总人口的百分比低于 20%。与之形成对比的是中国：互联网用户人数最多，在地图上“领土”最大；同时互联网用户人数占总人口的 40%-60%，“领土”颜色为橘红。

分布点越多，熵降低速度越快。所以中国拥有世界最多的互联网人口，理论上在中国的系统中熵降低速度会最快。若考虑人均在线时间，中国是美国 3 倍，这又是中国建立分布式系统，并健康运行的基础优势。

以上是从物理学、纯理论的角度分析区块链的应用，联系到实际情况，还需要一定的监管，才能用区块链的思维降低整个系统的熵。

投资建议

应用已开始

澳洲证券交易所：考虑使用区块链来替代清算和结算系统

澳洲证券交易所（ASX）正在认真考虑使用比特币背后的区块链技术，作为其清算和结算系统的替代品。

ASX 正在替换其交易系统的过程中，因为区块链能够降低清算和结算交易的成本和复杂性，并能节省下时间。而此前的这些工作，都是由清算所电子附属登记系统（CHESS）来完成的。ASX 已经建立了股票交易后系统，并将其作为一个独立的业务，要实现提升端到端之间交易的效率，为此，ASX 已经开始钻研区块链技术，探究它能够为我们的客户、投资者和企业创造些什么效益。

澳洲主要的银行已加入了全球金融创新公司 R3 运行的区块链项目，项目至今，已有 22 家全球银行的参与。R3 设计了一种协议，银行可能使用它，以较低的成本来传输资金或信息，并且也不必依赖于中央银行。ASX 正在考虑是否存在更棒的解决方案，它能够删除掉大量的管理成本，和投资银行业务和经济业务背后的和解费用，而这也是区块链的潜力所在。

区块链和类似的分布式总账，使用了先进的加密计算机技术来跟踪交易，因此，它能够绕过传统的银行或清算所。

央行开始研究数字货币

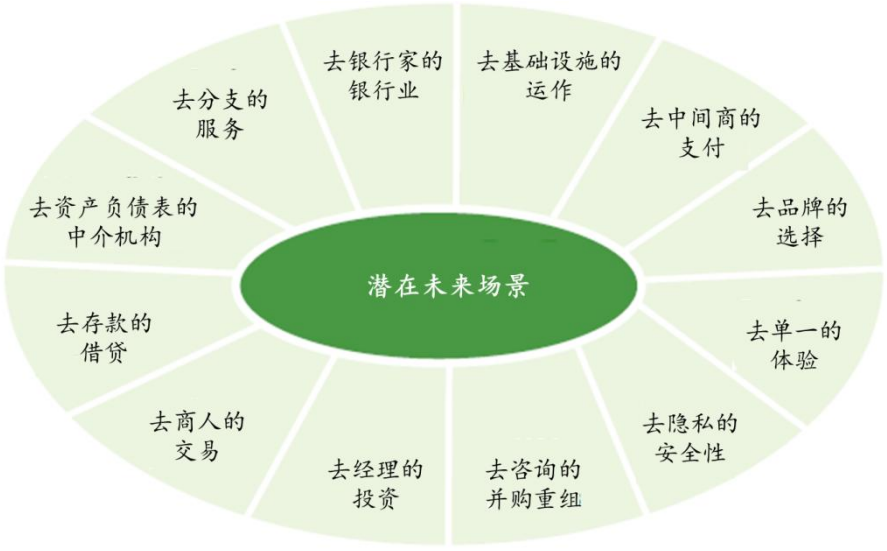
2016 年 1 月 20 日，中国人民银行数字货币研讨会提出，人民银行数字货币研究团队要积极吸收国内外数字货币研究的重要成果和实践经验，在前期工作基础上继续推进，建立更为有效的组织保障机制，进一步明确央行发行数字货币的战略目标，做好关键技术攻关，研究数字货币的多场景应用，争取早日推出央行发行的数字货币。2016 年 2 月 14 日，央行行长周小川对区块链的观点是“区块链技术现在肯定不行 以后行不行还不知道”。

未来银行业

未来十年我我们可以预想一个完全不同的产业竞争格局：拥有数字技术优势的新进入者会占据上风，而许多既有企业会被迫改变他们的竞争策略。结果是，产业会更加分裂并逐渐模糊产业边界，金融服务更多地会由新兴的非银行机构所提供。

为了预测银行业会被分裂到如何一种程度，我们重新想象一个颠覆传统的未来。图中某些场景只是遥远的设想，而有些或许在未来十年之内就会成为可能。

图 37：银行业潜在未来场景想象图



资料来源：Deloitte，国信证券经济研究所整理

路还很长

区块链已经受到当局重视，但是从一个新技术出现到大规模应用还有很长的路要走。

从二级市场投资角度看，A 股以及海外上市公司都没有区块链标的，该领域的创新和应用还在一级市场。从相关性上来看，A 股的一些安全概念股（涉及到密码）、征信概念股（未来信用）、大数据概念股（数据区块连接）。

国信证券投资评级

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

分析师承诺

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

风险提示

证券投资咨询业务的说明

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

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

国信证券经济研究所团队成员

宏观		策略		技术分析	
董德志	021-60933158	鄢　彬	021-6093 3155	闫　莉	010-88005316
陶　川	010-88005317	朱俊春	0755-22940141		
燕　翔	010-88005325	孔令超	021-60933159		
李智能	0755-22940456	王佳骏	021-60933154		
固定收益		**纺织/日化/零售**		**互联网**	
董德志	021-60933158	郭陈杰	021-60875168	王学恒	010-88005382
赵　婧	0755-22940745	朱　元	021-60933162	李树国	010-88005305
魏玉敏	021-60933161			何立中	010-88005322
柯聪伟	021-60933152				
医药生物		**社会服务(酒店、餐饮和休闲)**		**家电**	
江维娜	021-60933157	曾　光	0755-82150809	王念春	0755-82130407
邓周宇	0755-82133263	钟　潇	0755-82132098		
万明亮		张峻豪	0755-22940141		
通信服务		**电子**		**环保与公共事业**	
程　成	0755-22940300	刘　翔	021-60875160	陈青青	0755-22940855
李亚军	0755-22940077	刘　洵	021-60933151	邵　潇	0755-22940659
		蓝逸翔	021-60933164		
		马红丽	021-60875174		
军工及主题投资				**非金属及建材**	
梁　铮	010-88005381			黄道立	0755-82130685
王　东	010-88005309			刘　宏	0755-22940109
徐培沛	0755-82130473				
房地产		**食品饮料**			
区瑞明	0755-82130678	刘　鹏	021-60933167		
朱宏磊	0755-82130513				
电力设备新能源		**化工**		**建筑工程**	
杨敬梅	021-60933160	苏　淼	021-60933150	刘　萍	0755-22940678
金融工程		**轻工造纸**		**汽车及零部件**	
吴子昱	0755-22940607	邵　达	0755-82130706	梁　超	0755-22940097
黄志文	0755-82133928				
邹　璐	0755-82130833-701418				

国信证券机构销售团队

华北区（机构销售一部）	华东区（机构销售二部）	华南区（机构销售三部）	海外销售交易部
李文英 010-88005334 13910793700 liwying@guosen.com.cn	汤静文 021-60875164 13636399097 tangjingwen@guosen.com.cn	赵晓曦 0755-82134356 15999667170 zhaoxxi@guosen.com.cn	赵冰童 0755-82134282 13693633573 zhaobt@guosen.com.cn
夏　坤 13726685252	吴　国 15800476582	邵燕芳 0755-82133148 13480668226 shaoyf@guosen.com.cn	梁　佳 0755-25472670 13602596740 liangjia@guosen.com.cn
王　玮 13726685252	唐泓翼 13818243512	颜小燕 0755-82133147 13590436977 yanxy@guosen.com.cn	程可欣 886-0975503529(台湾) chengkx@guosen.com.cn
许　婧 18600319171	梁轶聪 021-60873149 18601679992 liangyc@guosen.com.cn	黄明燕 18507558226	刘　研 0755-82136081 18610557448 liuyan3@guosen.com.cn
边祎维 13726685252	倪　婧 18616741177	刘紫微 13828854899	夏　雪 18682071096
王艺汀 13726685252	林　若 13726685252	郑　灿 0755-82133043 13421837630 zhengcan@guosen.com.cn	
赵海英 010-66025249 13810917275 zhaohy@guosen.com.cn	张南威 13726685252	廖雯婷 13726685252	
	周　鑫 13726685252		