https://yq.aliyun.com/articles/60131

【第一篇】

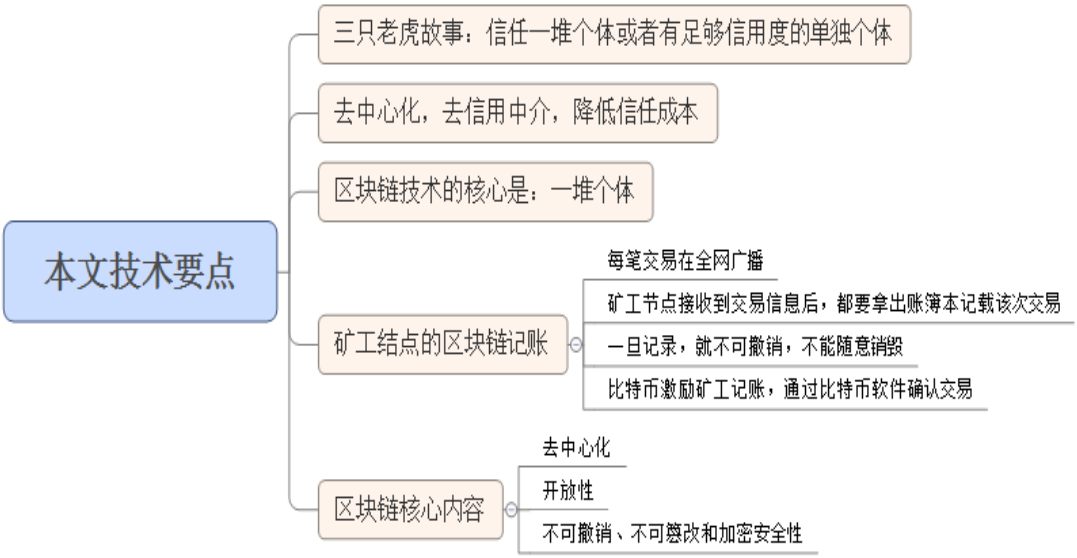
作为一枚软件专业的学生党而言，时刻关注互联网新趋势我们的必修课。毕竟呀，互联网这个行业，没有什么是永恒不变的，今天我们在课堂上学的技术，或许在未来就死掉了，所以从刚刚踏入大学校门的第一节课老师就告诫我们：**学不到老就活不到老。**互联网技术的发展远比其他行业的发展迅速得多，虽然工程理论已经很健全了，但是新技术和新概念却层出不穷，当今时代因为互联网，思维可以无限地碰撞，而撞出的火花就会诞生一门新技术。

前一段时间在做智能问答系统的创新项目，老师说要我们多关注 TensorFlow，沃森还有微软小冰这些问答系统，看他们是怎样实现的，我一开始就有个疑问，谷歌微软这些公司的一帮“大牛”在研究的事情，我们一群本科生还能研究出比人家更高、更快、更强的东西么？后来，老师的话却让我重新看待了这个问题，**其实很多技术我们现在不跟上，以后等新技术正真发展起来就永远只能望其项背了，如果我们现在关注这些新技术的发展，并且勇于尝试，哪怕是一点点，随着实践的积累和技术的发展，也有可能成为站在浪潮之巅的技术领导者。**

言归正传，最近“区块链”的概念可以说是异常火爆，好像互联网金融峰会上没人谈一谈区块链技术就 out 了，BAT 以及各大银行还有什么金融机构都在开始自己的区块链研究工作，就连 IBM 最近也成立了自己的区块链研究实验室，但其实区块链到底是什么？大家或许并不清楚，停留在雾里看花的状态。我呢，对于互联网金融更是非常感兴趣，看到互联网上那么多的文章，于是决心不再做收藏夹党，而是网罗精华文章，也为大家整理一个区块链学习系列，大家就和我一起走进区块链吧，揭开区块链的神秘面纱吧！**注意：前方高能预警！**

这篇文章是区块链学习进阶的第一部分：【区块链之菜鸟入门】的第一篇文章，先抛开技术细节，本文将以漫画的形式（有才！）让大家对于区块链有一个大致的印象。

本文技术要点：



那么，[谁叫的区块链，来门口取一下！]

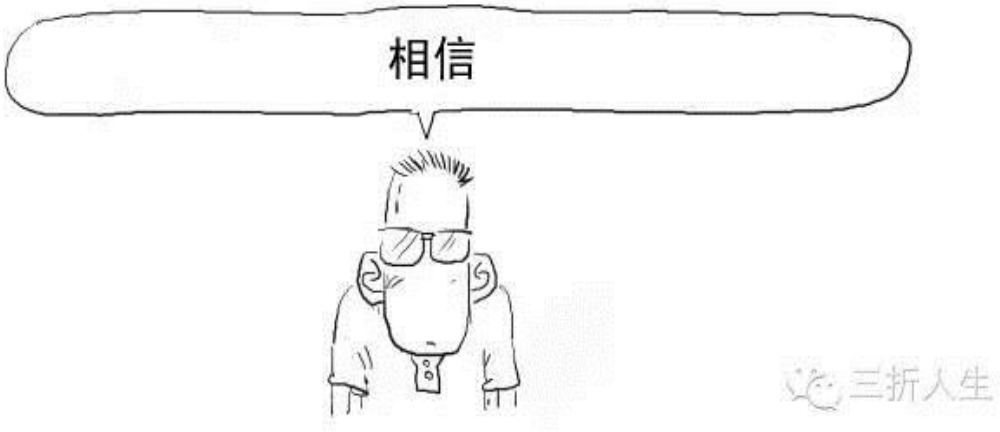
本文转载自：新金融　原文作者：**三折人生**　[原文链接]

取快链？你想说的是区块链吧？

要说清楚区块链，我们先来讲个故事。

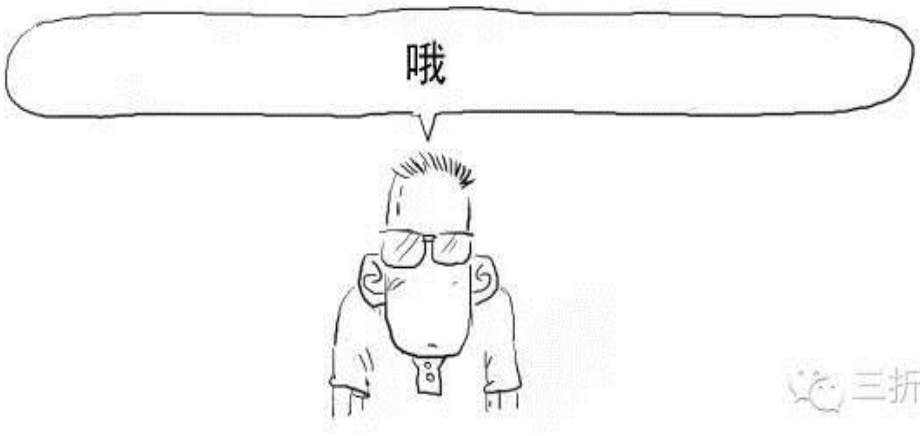
你一定听说过三人成虎的故事吧？

假设一个人告诉你，不好了，大街上有只老虎，你相不相信？



我去，你咋不按常理出牌啊，你要说不相信！

重来！我们说的是真老虎！



action！！

好！非常好！！影帝级的演出！！！

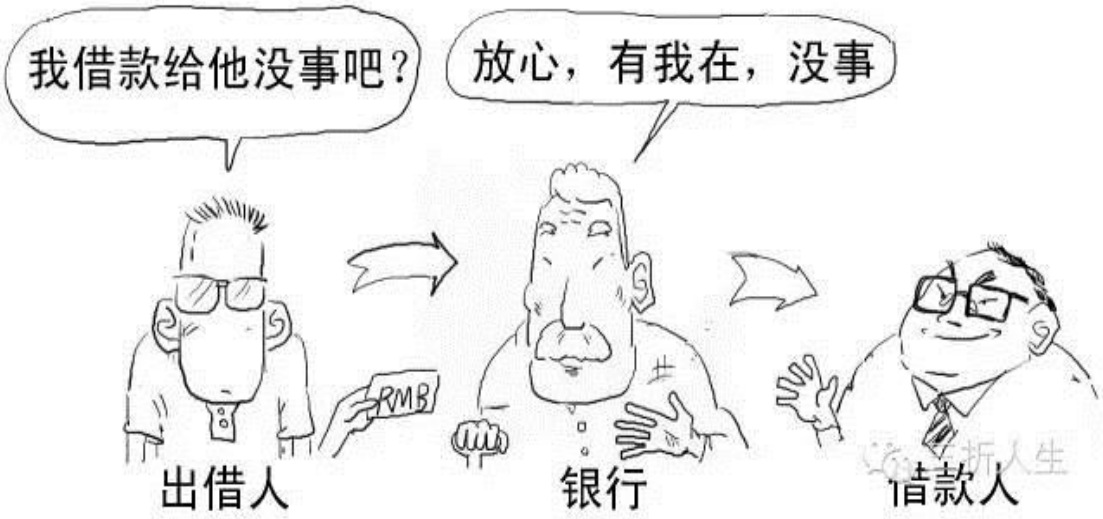
继续，这时候换做**一堆人**告诉你这件事！

我们再换一种场景。

如果一个德高望重、你**十分信任的老者**告诉你这件事，你又会怎么想？

是的，这就是所谓的信任的力量。你不信任一个没有足够信用度的单独个体，但你会信任**一堆个体**或者有**足够信用度的单独个体**。

在现实社会中，**银行就是这个有足够信用度的个体（中心）**。



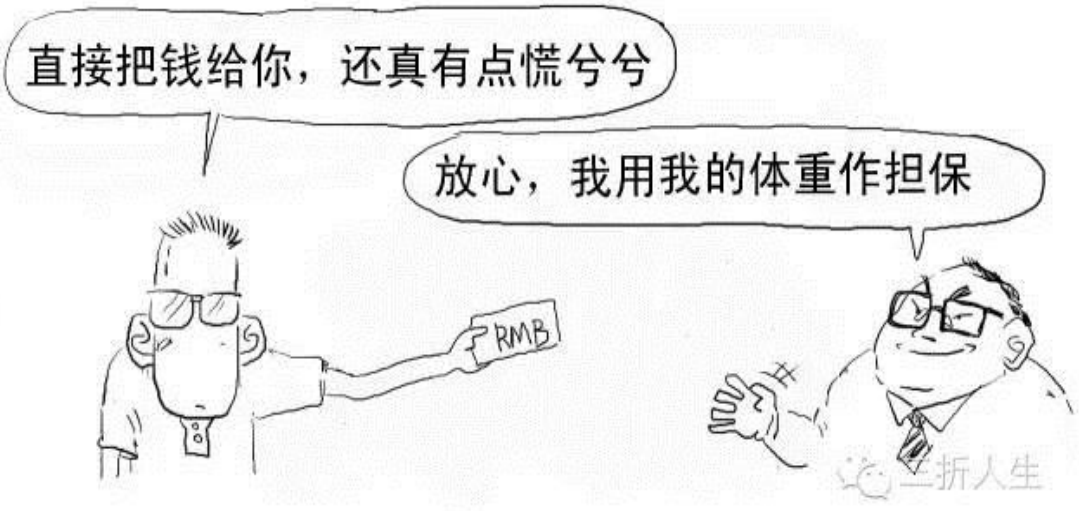
但以银行等作为信用中介是需要成本的，

而我们普通大众就要为这庞大的信用成本买单。

所以才会造就金融业是最赚钱的行业。

要去除银行类等中心机构的信用背书？

那就可以用我们上面提到过的**“一堆个体”**，这也是区块链技术的核心。



区块链**本质**上是解决信任问题、降低信任成本的技术方案，

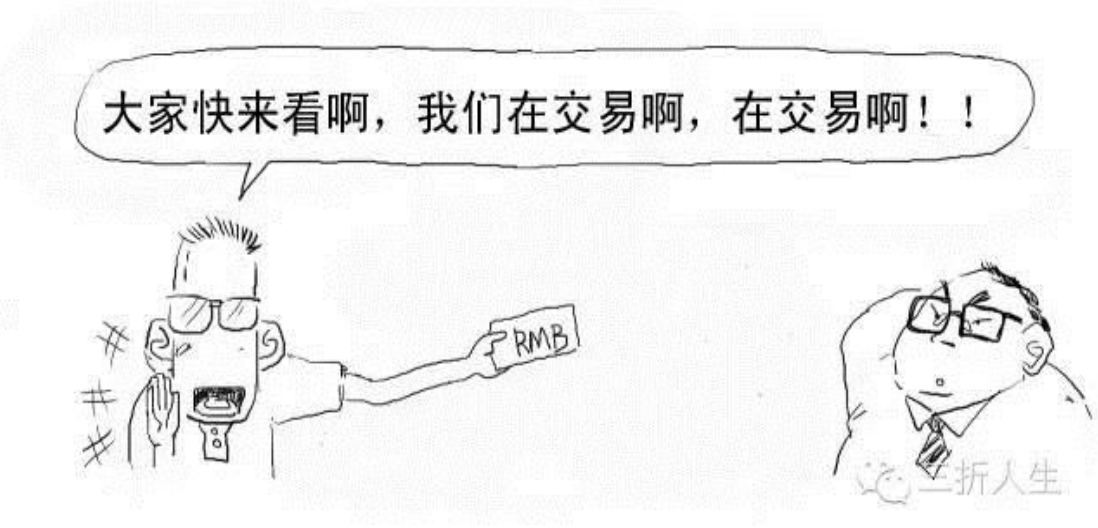
目的就是为了**去中心化，去信用中介**。

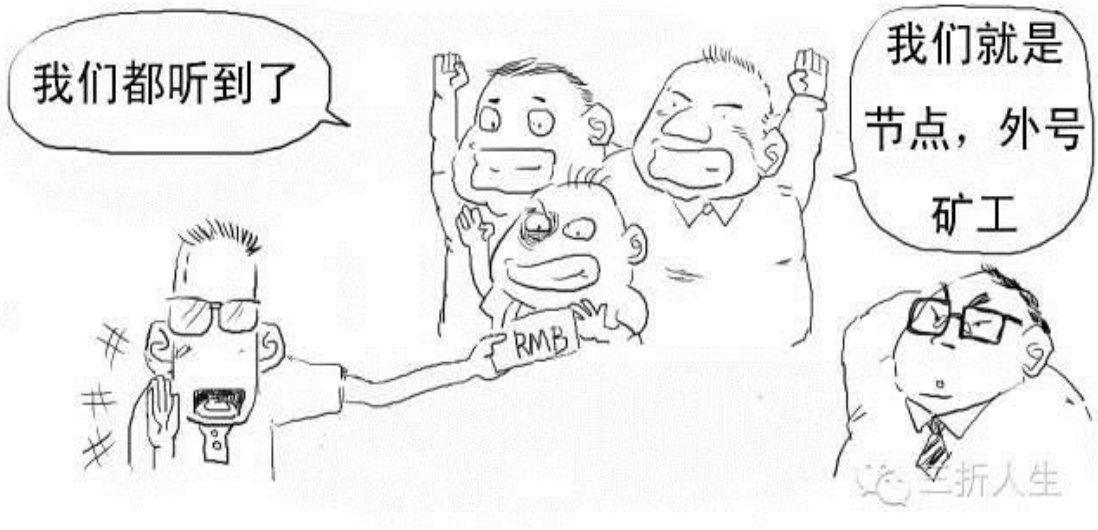
区块链是比特币的底层技术。

比特币（BitCoin）的概念最初由**中本聪**在 2009 年提出，你把它理解成数字货币即可。

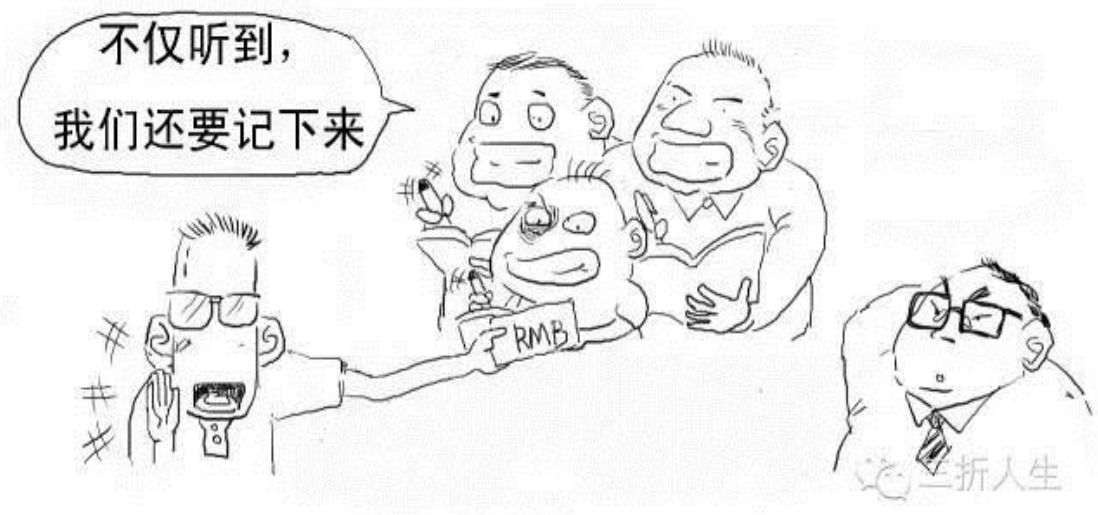
我们以比特币交易为例来看看区块链具体是如何操作的。

1、把每笔交易在全网广播。让全网承认有效，必须广播给每个节点。

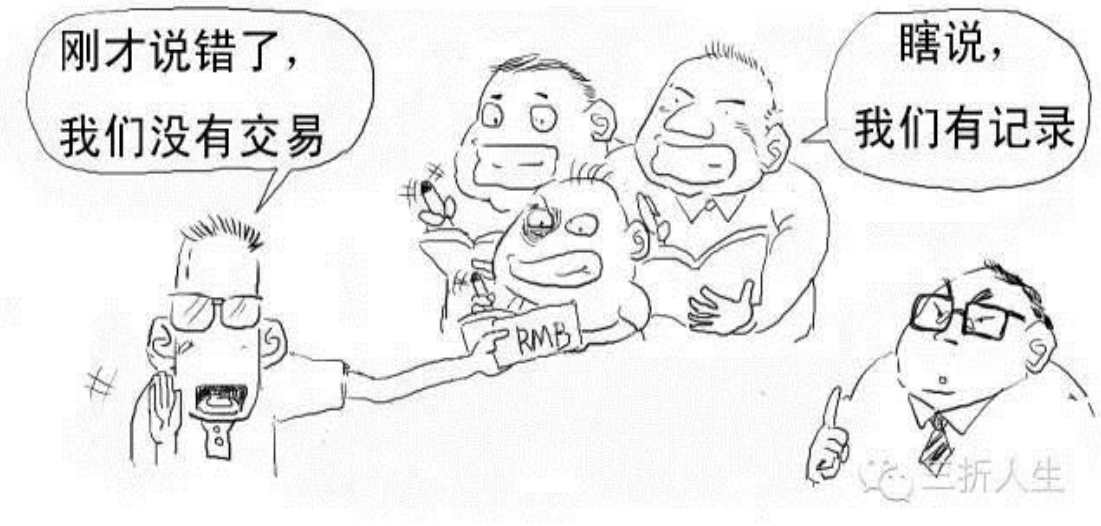




2、矿工节点接收到交易信息后，都要拿出账簿本记载该次交易。



一旦记录，就不可撤销，不能随意销毁。



矿工节点是通过电脑运行的比特币软件对交易的进行确认的。

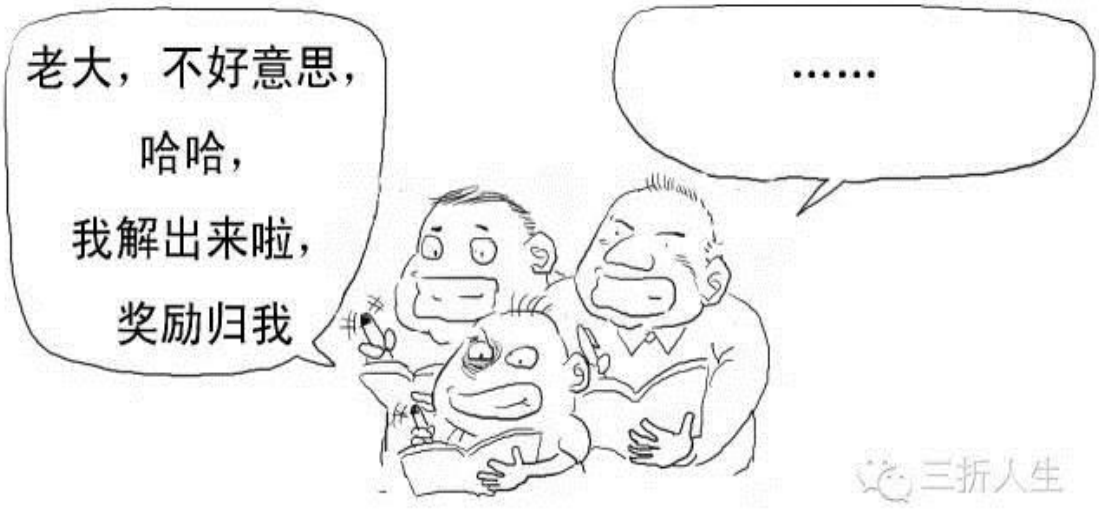
为了鼓励矿工的服务，对于其所记录和确认的交易，

系统为矿工提供 25 个比特币作为奖励。（这个奖励数量，系统设定每 4 年减半）

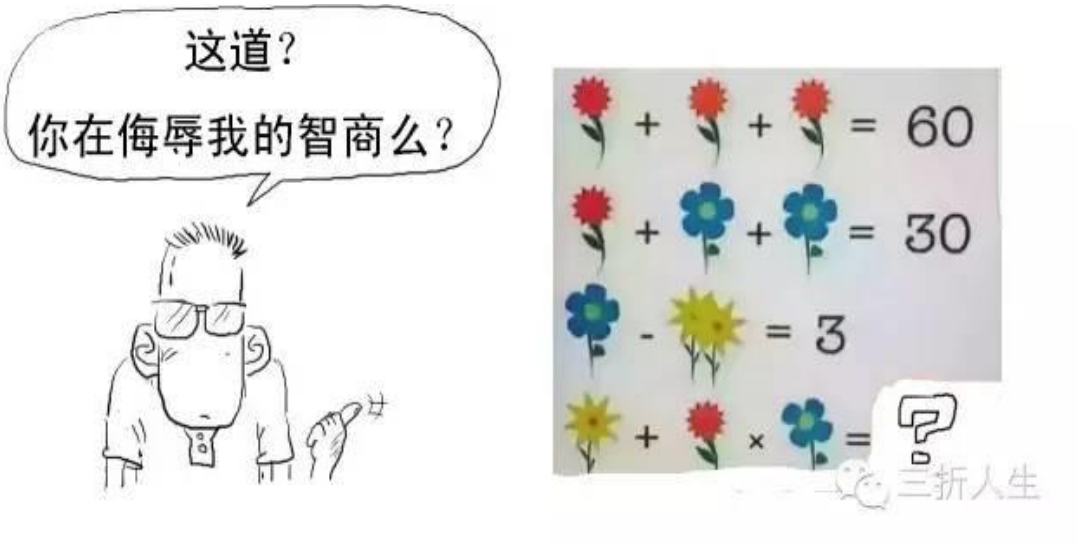
奖励只有一份，那就看谁记录的快呗。

为了减少这种情况，系统会出一道十分钟的运算题，

谁能最快解出值，谁就将获得记录入账权利，并赢得奖励。



对了，这里可以给大家看一道据说是徐汇区**幼儿园升小学**的运算题。

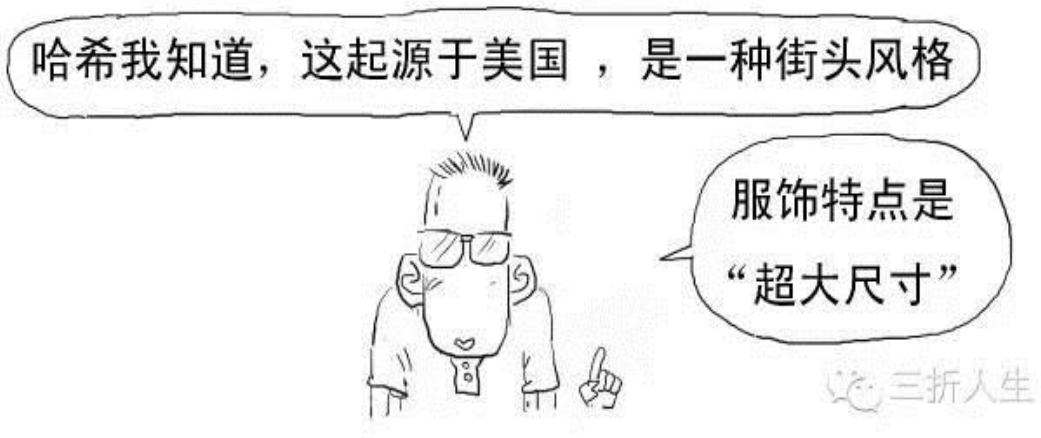


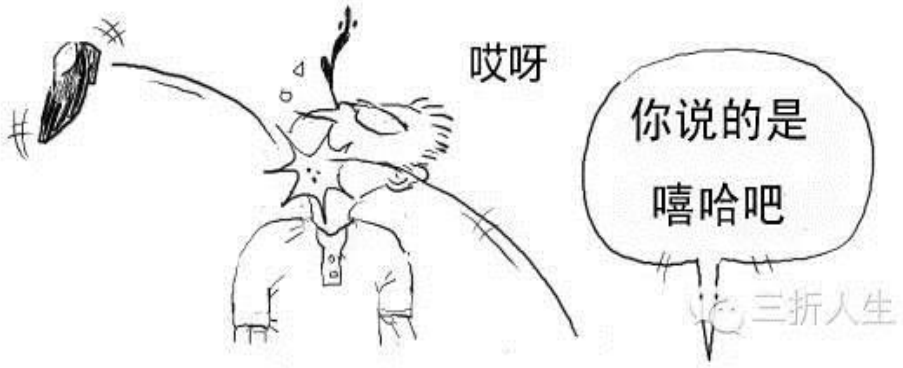
别急啊，你试试看，我第一次反正是做错了。

%&*%#@%，好吧，我无力反驳。

说远了，我们再说回来。

前述区块链中所运用算法并不是简单的计算题，而是使用**哈希散列（Hash）算法**。





哈希散列是密码学里的经典技术，可以用来验证有没有人篡改数据内容。

3、获得记账权的矿工将向全网广播该笔交易，账簿公开，其他矿工将核对确认这些账目。

交易达到 6 个确认以上就成功记录在案了。

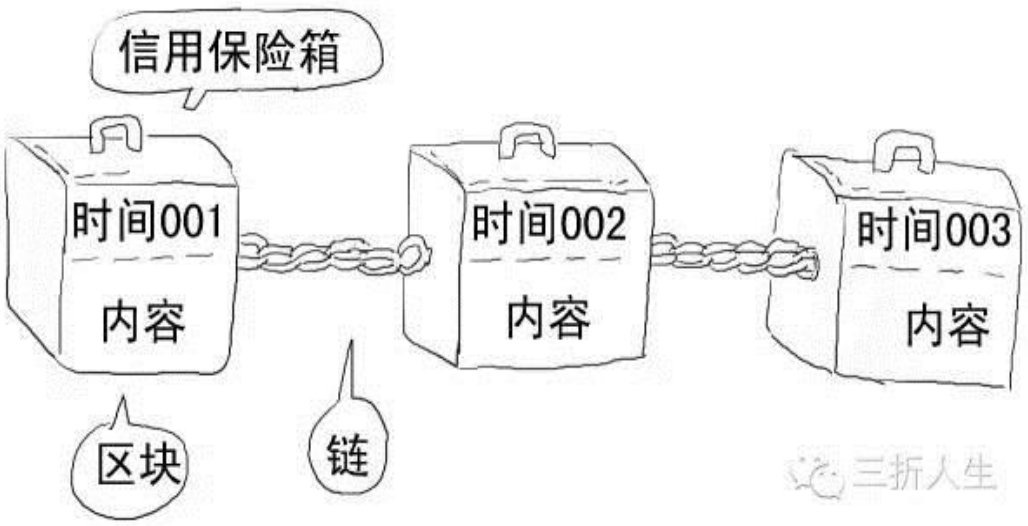
矿工记录的时候，还会将该笔交易盖上时间戳，形成一个完整时间链。

4、当其它矿工对账簿记录都确认无误后，该记录就确认合法，

矿工们就进入了下一轮记账权争夺战。

矿工的每个记录，就是一个**区块（block）**，会盖上**时间戳**，每个新产生的区块严格按照**时间线形顺序**推进，

形成不可逆的链条（chain），所以叫做区块链（Blockchain）。



而且每个区块都含有其上一个区块的哈希值，确保区块按照时间顺序连接的同时没有被篡改。

这时候我们再看对区块链的原始定义就能理解了：区块链是一种分布式数据库，是一串使用密码学方法相关联产生的数据块，

每个数据块都包含了一次网络交易信息，用于验证其信息的有效性和生成下一个区块。

若两个人同时上传，虽然这个概率很小，但是若发生，我们就看最后的区块链哪条更长，短的那条就失效。这就是区块链中的**“双花问题”**（同一笔钱花两次）。

对于要制作虚假交易，除非你说服了全网里超过 51%的矿工都更改某一笔账目，否则你的篡改都是无效的。

网络中参与人数越多，实现造假可能性越低。

这也是集体维护和监督的优越性，伪造成本最大化。

说服 51%的人造假还是灰常灰常难的。

是的。

好了，我们总结下，区块链主要有以下核心内容：

1、去中心化

这是区块链颠覆性特点，不存在任何中心机构和中心服务器，所有交易都发生在每个人电脑或手机上安装的客户端应用程序中。

实现点对点直接交互，既节约资源，使交易自主化、简易化，又排除被中心化代理控制的风险。

2、开放性

区块链可以理解为一种公共记账的技术方案，系统是完全开放透明的，

账簿对所有人公开，实现数据共享，任何人都可以查账。

开放效果类似这样：

3、不可撤销、不可篡改和加密安全性

区块链采取单向哈希算法，每个新产生的区块严格按照时间线形顺序推进，时间的不可逆性、不可撤销导致任何试图入侵篡改区块链内数据信息的行为易被追溯，

导致被其他节点的排斥，造假成本极高，从而可以限制相关不法行为。

【第二篇】

在“**【区块链之菜鸟入门】亲，你淘的区块链到了！**”这篇文章中，我们了解到了区块链技术的出现其实是为了去除银行类等中心机构的信用背书。从原本信任足够信用度的**单独个体（中心）**到信任**一堆个体，**这一过程就极大地降低了信任成本，而区块链技术的核心也就是**去中心化，去信用中介。**我们也聊到了区块链是比特币的底层技术，但是区块链就仅仅是比特币的底层技术么？区块链经过了怎样的变革才走到今天的呢？本文就为大家揭晓。

本文是【区块链之菜鸟入门】部分的第二篇，什么？拜占庭将军问题、杂凑现金……听上去蛮有意思，等着，我去搬个小板凳，听一听区块链的发展史中的那些事。

本文技术要点：

区块链源自**比特币**，不过在这之前，已有多项跨领域技术，皆是构成区块链的关键技术；而现在的区块链技术与应用，也已经远超过比特币区块链。要追溯**区块链（Blockchain）**是怎么来的，不外乎先想到**比特币（Bitcoin）**，比特币是第一个采用区块链技术打造出的 P2P 电子货币系统应用，不过比特币区块链并非一项全新的技术，而是将跨领域过去数十年所累积的技术基础结合。

比特币区块链所实现的基于**零信任基础、且真正去中心化的分散式系统**，其实解决一个 30 多年前由 Leslie Lamport 等人所提出的**拜占庭将军**问题。

1982 年 Leslie Lamport 把军中各地军队彼此取得共识、决定是否出兵的过程，延伸至运算领域，设法建立具容错性的分散式系统，即使部分节点失效仍可确保系统正常运行，可让多个基于零信任基础的节点达成共识，并确保资讯传递的一致性，而 2008 年出现的比特币区块链便解决了此问题。而比特币区块链中最关键的工作量证明机制，则是采用由 Adam Back 在 1997 年所发明 **Hashcash（杂凑现金）**，为一种**工作量证明演算法（Proof of Work，POW）**，此演算法仰赖成本函数的不可逆特性，达到容易被验证，但很难被破解的特性，最早被应用于阻挡垃圾邮件。

在隐私安全方面的技术，可回溯到 1982 年 David Chaum 提出注重隐私的密码学网路支付系统，具有不可追踪的特性，成为比特币区块链在隐私安全面上的雏形，之后 David Chaum 也基于这个理论打造出不可追踪的密码学网路支付系统 eCash，不过 eCash 并非去中心化系统。

在区块链中每笔交易，采用**椭圆曲线数位签章演算法（Elliptic Curve Digital Signature Algorithm，ECDSA）**，可追溯回 1985 年 Neal Koblitz 和 Victor Miller 分别提出椭圆曲线密码学（Elliptic curve cryptography，ECC），首次将椭圆曲线用于密码学，建立公开金钥加密的演算法。相较于 RSA 演算法，采用 ECC 好处在于可以较短的金钥，达到相同的安全强度。到了 1992 年，由 Scott Vanstone 等人提出 ECDSA。

区块链最早源于比特币，但区块链的应用却不仅于此。

过去几年也陆续出现许多基于区块链技术的**电子货币（统称为 Altcoins)**，不过随着比特币持续备受争议，各国政府与金融机构纷纷表态，直到近 1、2 年，大家才终于意识到区块链的真实价值，远超过于电子货币系统。

区块链可结合认许制，以满足金融监管需求

若要将比特币与区块链技术分开来看，最大的不同之处在于，由于比特币为虚拟货币应用，因此面临各国法规的限制，但区块链现在已经可结合认许制或其他方式来管控节点，决定让哪些节点参与交易验证及存取所有的资料，并提供**治理架构（Governance Structure）**及**商业逻辑（Business Logic）**两大关键特性。目前区块链可分为非实名制和实名制两种，前者如比特币区块链，后者如台大地的 GCoin 区块链。现在的区块链已经可结合**认许制 (Permissioned)**，来配合金融监管所需的**反洗钱 (AML) 与身份验证 (KYC)** 规范。而银行和金融机构想采用的都是实名制的区块链。

区块链演进阶段

区块链技术随着比特币出现后，经历了几个不同的阶段，常见的分法将比特币视为 Blockchain 1.0，为**数位货币（Currency）**应用，Blockchain 2.0 开始出现如**智慧资产（Smart Assets）、智慧契约（Smart Contracts）**等货币以外的应用，Blockchain3.0 则是指更复杂的智慧契约，将区块链用于政府、医疗、科学、文化与艺术等领域。

区块链新创 DTCO 执行长李亚鑫基于现有的分法进行补充，他认为，Blockchain 2.0 以彩色币（Colored Coin）为代表，在区块链上运行 Open Assets Protocal，可传递货币以外的数位资产，如股票、债券等。而从 Blockchain 2.0 之后，可再分出一类属于 Blockchain 2.5 的应用，包括**代币（货币桥）应用、分散式帐本（Distributed Ledgers）、资料层区块链（Data Layers Blockchain）、结合人工智慧（Artificial Intelligent）**，以及无交易所的国际汇款网路，以 Ripple 为代表，资料层、分散式储存则以 Factom、MaidSafe 为代表，Blockchain3.0 则以 Ethereum 为代表。他表示，Blockchain2.5 跟 Blockchain3.0 最大的不同在于，3.0 较强调是更复杂的智慧契约，以 2.5 则强调代币（货币桥）应用，如可用于金融领域联盟制区块链，如运行 1:1 的美元、日圆、欧元等法币数位化。由于区块链协议几乎都是开源的，因此要取得区块链协议的原始码不是问题，重点是要找到好的区块链服务供应商，协助导入现有的系统。而银行或金融机构得对区块链有一定的了解，才能知道该如何选择，并应用于适合的业务情境。去年**金融科技（Fintech）**才刚吹进亚洲，没想到才过几个月，一股更强劲的区块链技术也开始引爆，全球金融产业可说是展现了前所未有的决心，也让区块链迅速成为各界切入金融科技的关键领域。

尽管现在就像是区块链的战国时代，不过银行或金融机构要从理解并接受区块链，到找出一套大家都认可的区块链，且真正应用于交易上，恐怕还需要一段时间。这次只比国外晚了半年，引爆点可从台大释出一套自行开发的开源区块链协议 GCoin，并宣布将成立金融科技暨区块链中心说起，短短一周的时间，便引发各界高度关注，接着研讨会不断，不过，由于区块链具有较高的技术门槛，大家都知道它拥有许多特性跟好处，但却迟迟处于观望阶段，就连区块链的新创业者，也非常稀少。银行业目前也还卡在门口，除了少数金控开始分享这个议题之外，多数金融业者仍处于试图理解技术面的阶段。

技术演进：区块链是怎么来的

1982 年

- **拜占庭将军问题**
  Leslie Lamport 等人提出拜占庭将军问题（Byzantine Generals Problem），把军中各地军队彼此取得共识、决定是否出兵的过程，延伸至运算领域，设法建立具容错性的分散式系统，即使部分节点失效仍可确保系统正常运行，可让多个基于零信任基础的节点达成共识，并确保资讯传递的一致性，而 2008 年出现的比特币区块链便解决了此问题。
- **David Chaum 提出密码学网路支付系统**
  David Chaum 提出注重隐私安全的密码学网路支付系统，具有不可追踪的特性，成为之后比特币区块链在隐私安全面的雏形。

1985 年

- **椭圆曲线密码学**
  Neal Koblitz 和 Victor Miller 分别提出椭圆曲线密码学（Elliptic Curve Cryptography，ECC），首次将椭圆曲线用于密码学，建立公开金钥加密的演算法。相较于 RSA 演算法，采用 ECC 好处在于可用较短的金钥，达到相同的安全强度。

1990 年

David Chaum 基于先前理论打造出不可追踪的密码学网路支付系统，就是后来的 eCash，不过 eCash 并非去中心化系统。

Leslie Lamport 提出具高容错的一致性演算法 Paxos。

1991 年

- **使用时间戳确保数位文件安全**
  Stuart Haber 与 W. Scott Stornetta 提出用时间戳确保数位文件安全的协议，此概念之后被比特币区块链系统所采用。

1992 年

Scott Vanstone 等人提出椭圆曲线数位签章演算法（Elliptic Curve Digital Signature Algorithm，ECDSA）

1997 年

- **Adam Back 发明 Hashcash 技术**
  Adam Back 发明 Hashcash（杂凑现金），为一种工作量证明演算法（Proof of Work，POW），此演算法仰赖成本函数的不可逆特性，达到容易被验证，但很难被破解的特性， 最早被应用于阻挡垃圾邮件。Hashcash 之后成为比特币区块链所采用的关键技术之一。(Adam Back 于 2002 年正式发表 Hashcash 论文)

1998 年

- **Wei Dai 发表匿名的分散式电子现金系统 B-money**
  Wei Dai 发表匿名的分散式电子现金系统 B-money，引入工作量证明机制，强调点对点交易和不可窜改特性。不过在 B-money 中，并未采用 Adam Back 提出的 Hashcash 演算法。Wei Dai 的许多设计之后被比特币区块链所采用。
- **Nick Szabo 发表 Bit Gold**
  Nick Szabo 发表去中心化的数位货币系统 Bit Gold，参与者可贡献运算能力来解出加密谜题。

2005 年

- **可重复使用的工作量证明机制（RPOW）**
  Hal Finney 提出可重复使用的工作量证明机制（Reusable Proofs of Work，RPOW），结合 B-money 与 Adam Back 提出的 Hashcash 演算法来创造密码学货币。

2008 年

- **Blockchain 1.0：加密货币**
  数位货币与支付系统去中心化、比特币：Satoshi Nakamoto（中本聪）发表一篇关于比特币的论文，描述一个点对点电子现金系统，能在不具信任的基础之上，建立一套去中心化的电子交易体系。

2012 年

- **Blockchain2.0：智慧资产、智慧契约**
  市场去中心化，可作货币以外的数位资产转移，如股票、债券。如 Colored Coin 便是基于比特币区块链的开源协议，可在比特币在区块链上发行多项资产

2014 年

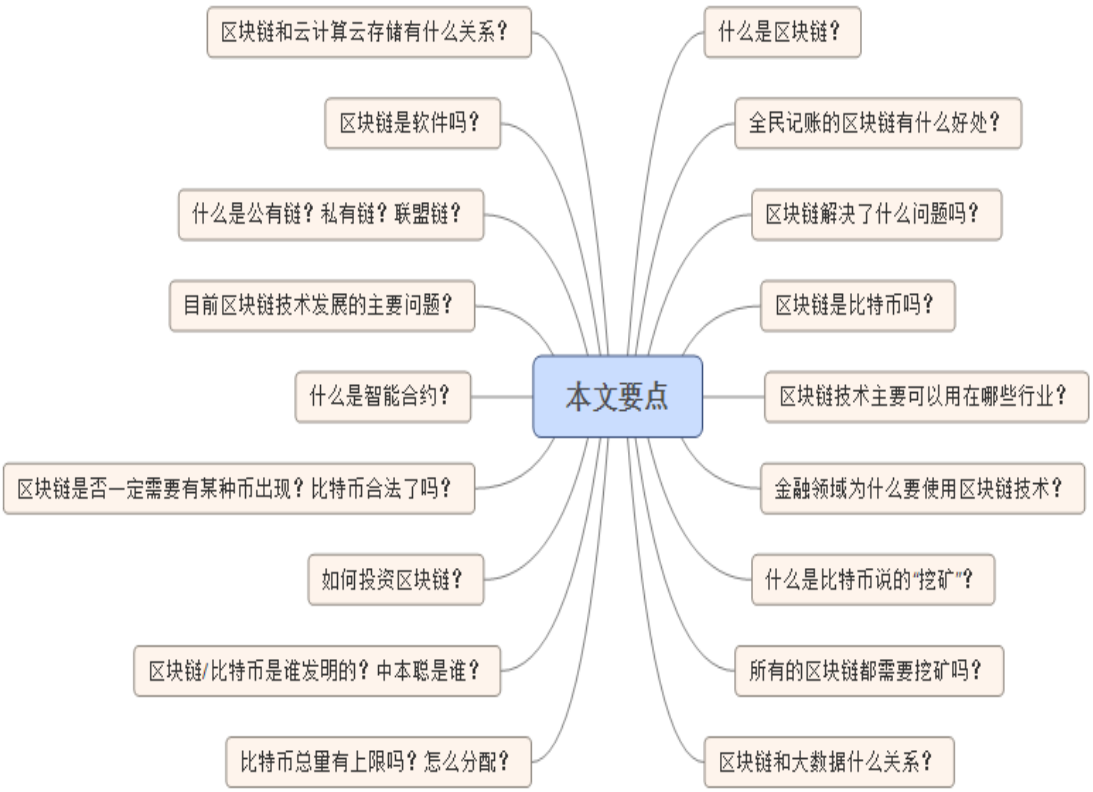
- **Blockchain 3.0：更复杂的智慧契约**
  更复杂的智慧合约，将区块链用于政府、医疗、科学、文化与艺术等领域。
  2016 年
- **Blockchain 2.5：金融领域应用、资料层**
- **Blockchain2.5：强调代币（货币桥）应用、分散式帐本、资料层区块链，及结合人工智慧等金融应用**
- **Blockchain 3.0：更复杂的智慧契约**

【第三篇】

通过前面的两篇文章相信大家已经对区块链技术有了一个大致的了解，对于区块链的技术发展史也有所涉猎。但是貌似还不是很明白，毕竟貌似区块链技术里还有很多的术语，对于这些术语，宝宝心里苦，但宝宝还要继续学习呀（哭笑脸）。不过呢，今天为大家分享的这篇文章偏科普性质，不需要大家对技术和金融有任何背景，会尽量回避一切技术术语，希望这篇文章能解决大家心里的一些疑惑所帮助。就算是小白的我也能读懂这篇关于区块链的文章呢，那你还在等什么？有了这篇文章，再约妹子吃饭，聊一聊区块链，瞬间逼格提升好几倍有木有？你还在等什么？看完记得给我点赞哈！

这篇文章是区块链学习进阶的第一部分：【区块链之菜鸟入门】的第三篇文章，本文将以一问一答的方式给大家送上一篇关于区块链的科普文。PS：区块链是比特币吗？金融领域为什么要使用区块链技术？所有的区块链都需要挖矿吗？区块链和大数据什么关系？...这些问题本文将会一一解答。**前方高能！**

本文要点



问：什么是区块链？

答：区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。通俗一点说，区块链技术就指一种全民参与记账的方式。所有的系统背后都有一个数据库，你可以把数据库看成是就是一个大账本。那么谁来记这个账本就变得很重要。目前就是谁的系统谁来记账，微信的账本就是腾讯在记，淘宝的账本就是阿里在记。但现在区块链系统中，系统中的每个人都可以有机会参与记账。在一定时间段内如果有任何数据变化，系统中每个人都可以来进行记账，系统会评判这段时间内记账最快最好的人，把他记录的内容写到账本，并将这段时间内账本内容发给系统内所有的其他人进行备份。这样系统中的每个人都了一本完整的账本。这种方式，我们就称它为区块链技术。

问：这样全民记账的区块链有什么好处？

答：可以发现，这是在牺牲一点效率的情况下，获得了极大的安全性。首先没有一本中央大账本了，所以无法摧毁。每个节点都仅仅是系统的一部分，每个节点权利相等，都有着一模一样的账本。摧毁部分节点对系统一点都没有影响。其次，无法作弊，因为除非你能控制系统内大多数人的电脑都进行修改，否则系统会参照多数人的意见来决定什么才是真实结果，结果会发现修改自己的账本完全没有意义（因为别人不承认）。其次，由于没有中心化的中介机构存在，让所有的东西都通过预先设定的程序自动运行，不仅能够大大降低成本，也能提高效率。而由于每个人都有相同的账本，能确保账本记录过程是公开透明的。

问：区块链解决了什么问题吗？

答：区块链最重要的是解决了中介信用问题。在过去，两个互不认识和信任的人要达成协作是难的，必须要依靠第三方。比如支付行为，在过去任何一种转账，必须要有银行或者支付宝这样的机构存在。但是通过区块链技术，比特币是人类第一次实现在没有任何中介机构参与的情况下，完成双方可以互信的转账行为。这是区块链的重大突破。

问：区块链是比特币吗？或者比特币就是区块链吗？

答：区块链技术是比特币的底层技术，在早期并没有太多人注意到比特币的底层技术。但是当比特币在没有任何中心化机构运营和管理的情况下，在多年里非常稳定的运行，并且没有出现过任何问题。所以很多人注意到，该底层技术技术也许有很大的机制，而且不仅仅可以在比特币中使用，也许可以在许多领域都能够应用这种技术。于是把比特币技术抽象提取出来，称之为区块链技术，或者分布

式账本技术。所以从某个角度来看，比特币可以看成是区块链第一个应用，而区块链更类似于 TCP/IP 这样的底层技术，以后会扩展到越来越多的行业中。

问：区块链技术主要可以用在哪些行业？

答：区块链主要的优势是无需中介参与、过程高效透明且成本很低、数据高度安全。所以如果在这三个方面有任意一个需求的行业都有机会使用区块链技术。

问：金融领域为什么要使用区块链技术？有什么实质性的好处？

答：区块链技术在金融领域中主要的优势去中介化和极大的降低成本。

首先金融行业目前由于防止单点故障和系统性风险，需要进行层层审计来控制金融风险，但由此也造成高昂的内部成本。并且由于不断增加的监管法规出现，特别是 2008 年金融危机导致对于金融管控门槛不断升高，而反恐战争导致反洗钱和反恐怖主义融资的范围也让监管的广度和深度逐渐扩大，导致整个金融系统的监管成本急剧增加。在这种情况下，区块链技术能够通过防篡改和高透明的方式让真个金融系统极大的降低成本。根据西班牙最大银行桑坦德发布的一份报告显示，2020 年左右如果全世界的银行内部都使用区块链技术的话，大概每年能省下 200 亿美元的成本。这样的数据足以说明“区块链”给传统金融领域带来的巨大变革和突破。

此外由于历史原因，导致传统金融机构在结算和清算时都依靠中央结算所来完成，而由此造成的问题就是效率低下。传统的跨国结算就是因为要通过类似于 SWIFT 这样的机构，所以跨国电汇往往是按天来计算的。但是比特币在使用区块链技术时，在完全没有中心化运营机构的情况下，完美的运行了七年，不仅能够实现实时结算和清算，而且没有出现过任何一笔账目错误。所以，如果所有的金融系统能够实现去中心化的实时结算和清算，不仅仅将极大的提高全球金融效率，并且由此能够改变全球金融的格局。

问：什么是比特币说的“挖矿”？

答：比特币中的“挖矿”实际上就是记账的过程，比特币的运算采用了一种称为“工作量证明（Proof of Work，PoW）”的机制，系统为了找出谁有更强大的计算能力，每次会出一道数学题，只有最快解出这道题目的计算机才能进行记账。而抢到记账权的计算机会获得 25 个比特币的奖励。通常把这个行为称为“挖矿”，把获得的比特币视为挖矿成功获得的奖励。

问：所有的区块链都需要挖矿吗？

答：并非所有的区块链项目都会采用类似于比特币这样的“工作量证明”方式，这更多出现在早期的区块链项目中。如果采取其他的证明机制，如“权益证明（Proof

of Stake，PoS）”、“股份授权证明机制（DPoS，Delegate Proof of Stake）”都是不需要采取这样的挖矿方式。

问：区块链和大数据什么关系？区块链会取代大数据？
答：区块链和大数据关系并不是很大。大数据主要的是对于海量数据进行管理，而区块链的核心是在没有中心化中介计入的情况下实现数据的高安全性和高可靠性。所以区块链和大数据并不互相冲突，也不会取代，完全是面对不同场景情况下对于数据的不同解决方案。

问：区块链和云计算云存储有什么关系？区块链是云计算或云存储吗？
答：云计算通常定义为通过互联网来提供动态易扩展且经常是虚拟化的资源，但是提供云计算平台的往往是一个中心化机构。而区块链组成的网络一般是没有特定的机构，所以区块链更接近分布式计算系统的定义，属于分布式计算的一种。不过，区块链是能够实现云存储的，不同于目前中心化提供云存储空间，区块链有一些提供去中心化的云存储方案。这样的项目包括 Storj，Sia，Maidsafe。

问：区块链是软件吗？是用什么程序写的？
答：区块链不是一种特定的软件，就像“数据库”这个三个字表现的意思一样，它是一种特定技术的设计思想。可以用绝大多数语言来实现它，而且实现的方式也有许多种。而且区块链技术目前还在快速发展中，相对而言，目前区块链技术设计思想还是比较简单的，也许在未来会变得愈加复杂。

问：什么是公有链？什么是私有链？什么是联盟链？
答：公有链是任何节点都是向任何人开放的，每个人都可以参与到这个区块链中参与计算，而且任何人都可以下载获得完整区块链数据（全部账本）。但是有些区块链的应用场景下，并不希望这个系统任何人都可以参与，任何人都可以查看所有数据，只有被许可的节点才可以参与并且查看所有数据。那么这种区块链结构我们称为**私有链**。

联盟链是指参与每个节点的权限都完全对等，大家在不需要完全互信的情况下就可以实现数据的可信交换，R3 组成的银行区块链联盟要构建的就是典型的**联盟链**。

但是随着区块链技术的快速发展，不排除以后公有链和私有链的界限会变得比较模糊。因为每个节点的可以有较为复杂的读写权限，也许有部分权限的节点会向所有人开发，而部分记账或者核心权限的节点只能向许可的节点开放，那就会不再是纯粹的公有链或者私有链。

问：目前区块链技术发展的主要问题？
答：目前区块链技术还处于一个非常早期的阶段，不仅尚未形成统一的技术标准，而且各种技术方案还在快速发展中。但是过去被认为基于区块链技术的系统会非常耗费资源（类似于比特币），或者区块链技术的系统处理数据有限制之类的问题已经在技术上获得了突破。但是，对于区块链技术的可扩展性，还没有经过大规模的实践考验，而现在主要还停留在原型设计阶段。

如果不能定量分析，使用区块链技术能够为我们带来的实际好处，包括能够节省的资金和创造的价值，那么金融行业短期内还会保持相对谨慎的态度。毕竟，目前全球金融的基础设施投入已经超过数万亿，要建立一套全新的金融架构和底层操作体系是需要有实际数据相支撑的。在现有技术还没有被部署并且获得使用案例的情况下，能节省下的总金额还是很难确定的。这到目前为止，还是一个巨大的疑问存在，就是到底需要多少资金才能建立一个足够强大的区块链来平台处理，资本市场生态系统每天需要面对的万亿数量级的美元。

此外区块链行业极其缺乏人才，**缺少大量既了解区块链技术，又了解金融的多方面人才，市场正在拼命寻找可以连接两个世界的人才，需要能够在现实世界中，将区块链技术能够在资本市场中实现，并且实现更好的功能。而需要建立基于区块链技术的全新系统，必然是需要这样的跨界人才。**

问：什么是智能合约？
答：智能合约是一种用计算机语言取代法律语言去记录条款的合约。智能合约可以由一个计算系统自动执行。如果区块链是一个数据库，智能合约就是能够使区块链技术应用到现实当中的应用层。传统意义上的合同一般与执行合同内容的计算机代码没有直接联系。纸质合同在大多数情况下是被存档的，而软件会执行用计算机代码形式编写的合同条款。智能合约的潜在好处包括降低签订合约、执行和监管方面的成本；因此，对很多低价值交易相关的合约来说，这是极大降低人力成本。

问：智能合约怎么用？
答：央行如果能够通过区块链来发行法币，那么也可以通过智能合约技术，将代码嵌入到法币发行的行为中，则这部分法币可以被称为**“可编程货币”**。比如，如果央行指定某一部分资金是发放到农业相关的账户，那么则可以对这部分资金写入相应程序，指定该部分资金只能进入到农业相关的账户中，那么这部分资金在任何情况下也不可能会被挪用到其他的账户中。如果大部分货币都成为“可编程货币”，那么我们则可以想象到，他们组成的金融环境就变成了**“可编程金融”**。

问：区块链和普通人有什么关系？
答：基本上没什么关系，除非是准备从事这方面的创业。就和 TCP/IP 协议和普通人之间的关系，普通人完全不需要知道什么是互联网底层的 TCP/IP 协议，只要享受互联网提供的服务就行。

问：区块链项目是否一定需要有某种币出现？
答：不是。比特币本身是作为一种支付系统，所以它需要有一个价值度量的工具，所以必须要有 bitcoin 出现。此外，为了奖励有更多人愿意贡献自己的计算机来为系统提供计算，所以需要有 bitcoin 来进行奖励。而在一些私有链的系统，可以设计专门的资产进行交易，而每个节点都是必须参与计算，这是他们的责任也是他们的权利，所以不用考虑通过奖励的方式来鼓励他们参与，所以在这样的系统里面就可能不再需要设计某种币的存在。

问：比特币现在合法了吗？

答：比特币在主要的世界大国，包括中国在内一直都是完全合法的。由于某些不良媒体的误导，使很多人以为中国曾经宣布过比特币非法。事实上，根据 2013 年 12 月 5 日，中国人民银行等五部委发布的防范比特币风险的通知中明确规定，比特币是一种特定虚拟商品，普通民众在自担风险的前提下拥有参与的自由。而各类金融机构和支付机构不得开展比特币相关的金融服务，或者将比特币作为投资标的。比特币在德国作为货币单位，在美国定义为大宗商品。欧盟法院认为比特币为一种支付手段，无需征收增值税。

问：XX 币可以投资吗？是区块链项目吗？是传销吗？
答：目前包括比特币在内的所有数字货币都具有很高的风险，区块链技术本身在刚刚起步阶段，所有的区块链项目也都具有非常高的风险。不建议任何普通人投资任何数字货币和区块链相关的项目。并且数字货币和区块链具有一定的技术门槛，普通人无法区分哪些是真实的项目，哪些是传销项目。所以普通人建议不要投资任何这类的项目。对于任何你无法分辨是否是传销的项目，请直接视为传销项目。

问：如何投资区块链？
答：大多数区块链都处于起步阶段，而主要都是在海外，国内好的区块链项目非常非常少，所以不建议任何非专业人士投资区块链项目。如果对区块链技术很有兴趣，自己有技术或者金融相关的背景，建议可以考虑在这方面进行创业。

问：区块链/比特币到底是谁发明的？中本聪是不是日本人？是不是美国政府的阴谋？
答：比特币是一个自称为“中本聪”的人或者团队创造的，并且在比特币项目初期就已经完全退出了这个项目。“中本聪”是日本人的可能性非常小，因为他过去的电子邮件中可以推测出，他应该是一个以英语为母语的人。此外比特币创造者对于目前比特币的项目已经完全没有影响力，所以不太可能是某个阴谋的产物。无论“中本聪”在之后是否会出现，或者在肉体上被消灭都无法影响对比特币产生太多的影响。

问：比特币和 Q 币到底有什么区别？
答：Q 币是一种中心化的电子货币，包括总量，发行方式都是由腾讯公司控制的。而比特币的总量，发行方式都是由程序和加密算法预先设定后，在全世界的多个节点上运行，没有任何人和机构可以修改，不受任何单一人或者机构来控制。一般称 Q 币为电子货币，或者企业代币。称比特币为数字货币或者加密数字货币。

问：比特币总量是有上限的吗？是怎么分配的？
答：如同前面所说，矿工参与争夺记账权是有机会获得奖励的。在开始的时候是每 10 分钟系统会奖励记账最快最好的人 50 个比特币，然后这 50 个每四年减半，差不多在 **2140 年**的时候就不再有新的比特币出现，将会达到 2100 万个的上限。在这之后，将会使用交易手续费来奖励矿工。

【第四篇】

区块链技术可以说在近期获得了大量的关注，小川行长公开表示央行要研究区块链技术；2015 年区块链成为了美国创投中获得融资最高的板块；26 岁少年 Vitalik 创建的开源区块链平台以太坊，2015 年 7 月上线后市值飙升至 10 亿美元，成为新晋独角兽。区块链在**金融、共享经济、物联网**等方面存在很高的应用价值，吸引了**高盛、花旗、纳斯 达克、德勤、Airbnb** 等巨头的积极布局。

这篇文章是区块链学习进阶的第一部分：【区块链之菜鸟入门】的第四篇文章，通过前几篇文章的分享，想必大家对于区块链技术的基础知识有了一个大致的了解，积累了一定的知识和概念，这时有同学会问了：区块链技术有哪些特点？有人说区块链可以称之为颠覆性创新技术，颠覆性在哪？创新又在哪呢？区块链的应用价值在哪些方面呢？其应用潜力又有多大呢？现阶段的区块链技术又有什么缺陷呢？本文不容错过！

本文要点

1、区块链是什么？

区块链本质上是一个去中心化的分布式账本数据库，是比特币的底层技术，和比特币是相伴相生的关系。区块链本身其实是一串使用密码学相关联所产生的数据块，每一个数据块中包含了多次比特币网络交易有效确认的信息。每当有加密交易产生时，网络中有强大运算能力的矿工(Miner)就开始利用算法解密验证交易,创造出新的区块来记录最新的交易。新的区块按照时间顺序线性地被补充 到原有的区块链末端,这个帐本就会不停的增长和延长。

通过复杂的公共钥匙和私人钥匙的设置，区块链网络将整个金融网络的所有交易的账本实时广播，实时将交易记录分发到每一个客户端中，同时还能保证每个人只能对自己的财产进行修改。当然，账本里也有别人的交易记录，虽然你可以看到数值和对应的交易地址（基本上这是由一段冗长的乱序字母和数字组成），但是如果不借用其他技术手段你也根本无法知道交易者的真实身份。（**可以通过访**

问 blockchain.info 来体验一下全球比特币交易平台的运作，对区块链技术获得一个更直观的了解。）

2、区块链技术具有哪些优点？

（1)分布式去中心化：区块链中每个节点和矿工都必须遵循同一记账交易规则，而这个规则是基于密码算法而不是信用，同时每笔交易需要网络内其他用户的批准，所以不需要一套第三方中介结构或信任机构背书。

在传统的中心化网络中，对一个中心节点（比如说，支付中介第三方）实行有效攻击即可 破坏整个系统，而在一个去中心化的，比如说区块链网络中，攻击单独一个节点是无法控制或破坏整个网络的，掌握网内 50%的节点只是获得控制权的开始而已。

（2） 无须信任系统：区块链网络中，通过算法的自我约束，任何恶意欺骗系统的行为都会 遭到其他节点的排斥和抑制，因此，区块链系统不依赖中央权威机构支撑和信用背书。传统的信用背书网络系统中，参与人需要对于中央机构足够信任，随着参与网络人数增加，系统的安全性下降。和传统情况相反，区块链网络中，参与人不需要对任何人 信任，但随着参与节点增加，系统的安全性反而增加，同时数据内容可以做到完全公 开。

（3）不可篡改和加密安全性：区块链采取单向哈希算法，同时每个新产生的区块严格按照时间线形顺序推进，时间的不可逆性导致任何试图入侵篡改区块链内数据 信息的行为都很容易被追溯，导致被其他节点的排斥，从而可以限制相关不法行为。

3、比特币区块链目前存在哪些缺陷？

比特币在经历了 5 年的发展后，目前市值达到 70 亿美元，接近一个中小型国家的 GDP，比较大的市值提供了较好的流动性保证。 但是也暴露了很多问题，例如：

（1）价格呈现高波动性，比特币炒作性强，但同时 又受制于监管限制，所以风险较大；

（2)交易费用升高，虽然比特币交易费用很低， 但随着交易变频繁，币值上涨，交易成本也大幅提高；

（3）容量限制。比特币区块 链设计之初人为地将一个区块容量设置为 1MB，随着交易量加大，容量开始面临限 制，处理速度受到影响。

（4）确认时间变长，由于容量限制和工作量证明时常挑战 运算极限，目前比特币无法处理超过每秒 7 次的交易，无法和类似 Visa 等支付方式 在速度这个纬度上进行抗衡。

（5）比特币由于隐蔽性强，所以在贩毒、军火交易、 支付绑架赎金等方面被广泛应用，同时前段时间人民币贬值期间，比特币也被用作进 行外汇转移。所以大部分国家的监管层比较难接受比特币的广泛应用。

4、各种形式的区块链创新

创新式区块链技术的出现和成熟，让产业内开始将焦点放至区块链技术其本身。首先，部署方式区块链出现创新，在比特币这种公共链（所有人都 可参与）形式的基础上，目前延伸出了联盟链和私链。这些链在信息公开程度和中心控制力度方面有所限制。

（1）联盟链采取多中心式，参与成员是预先根据一定特征 所设定的（比如说，各券商的策略分析师）。联盟链容易进行控制权限设定，拥有更 高的应用可扩展性，对于产业内（例如各券商）或跨国家同联盟机构的交易、清算、 结算、审计等都有很大的应用价值。

（2）私有链没有去中心，但具有分布式特点。 中心控制者指定可以参与和进行交易验证成员的范围。私有链对于公司政府内部的审 计和测试有很大的价值。

（3）比特币的缺点开始暴露后，大量的竞争币也开始出现， 拓展区块链技术应用范围。例如 Ripple，全球第一个开放的全球银行汇款和支付系统，核心是基于比特币区块链去中心化思想基础之上的 Ripple 支付协议，从而挑战传统的银行间 SWIFT 系统。

在 Ripple 系统中，比特币等虚拟货币、以及美元、欧元、 人民币等实体货币皆可流通并受到系统支持。Ripple 币为系统提供流动性和安全性。而作为另类区块链中的优秀改进，以太坊近日快速崛起，关键在于它将区块链和智能 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超强图灵完备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应用空间，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**。

5、区块链的应用价值和潜力有多大？

以目前的发展来看， 区块链技术在支付、金融交易、物联网等多领域存在广大应用潜力，其中智能合约是关键。支付方面，传统支付采用“拉式”模式（传统拉式是用户将个人信息提供给 第三方，第三方利用这些信息进行支付处理），而区块链技术采用“推式”模式，直接绕开第三方，大幅改善安全性。

同时区块链自动化强降低支付成本并缩短处理时间， 去中心化开放特点则有助于平台内创新。智能合约作为区块链延伸核心技术打开区块 链各种领域互联智能的应用空间。

在金融交易领域，区块链技术可将结算审核时间从小时级降低至秒级，自动化强大幅降低中间成本，结合智能合约将数字证券自动发行和金融衍生品交易变为可能。

在审计方面，公司不需要招聘专门审计人员来公司内部审核账本，所有交易可以集中记录储存在内部区块链，由于区块链具有不可逆性和时 间邮戳功能，会计事务所等外部审计人员和监管机构通过跟踪这些区块链可以实时监控公司账本，同时机构可以借此大幅减少对于审计员审核金融交易的依赖，将审计业 务变得更有效率。

对于物联网，智能设备呈现呈数量指数级增长，区块链技术在这些设备之间建立了低成本的互相直接沟通桥梁，同时又通过去中心化的共识机制提高系统的安全私密性。区块链叠加智能合约技术可将智能设备变成可以自我维护调节的独立个体，这些个体可在事先规定或植入的规则合约基础上执行类似和其他个体交换信息或核实身份等功能。

6、区块链产业目前处于怎样的发展阶段？

发达国家积极布局区块链，各领域多点开花。随着比特币的局限性开始显露，区块链技术结合智能合约的应用空间打开、优点开始展现，产业内投资重点已从比特币挖掘硬件转向区块链技术相关应用。目前最高融资区块链公司已超过 1 亿美元，而且很多初创公司目前正在雄心勃勃进行支付、交易、风控等多领域布局。

金融机构例如高盛、花旗、纳斯达克 等积极探索区块链在金融领域的应用，同时大力布局金融交易清算相关区块链技术公司，先行者纳斯达克已开始利用区块链技术进行私有股权发行交易；物联网和网络安全相关公司比较容易得到政府和大型机构投资者青睐；支付领域则得到银行和电商的垂青。需要注意的是，四大（德勤和普华永道）在区块链技术在审计领域的应用探索是非常积极的。

中国相关机构产业内投资力度较小，后期有望突破。我国过往的产业内相关投资较重视挖矿，以及报价、信息提供业务和咨询，商业模式比较简单。有深入商业模式研究、有一定规模的应用项目是比较匮乏的。

目前，行业内开始呈现出向区块链商业应用和深度探索的发展和投资趋势，但体量较小并且缺乏大型金融机构政府支持。万 向集团下的区块链实验室是比较少有的有大型机构支撑的研发项目，万向集团旗下还有区块链基金。其中万向集团相关负责人是肖风先生，也就是博时基金的前总经理。

随着央行对区块链重视加深、来自国外最新科技进展的溢出效应、海外以太坊作为区块链技术标准的逐渐确认、伴以区块链应用的更加成熟和可投资投标的增加，区块链有望成为“互联网+”后的下一个热捧对象。这将激发创业者和应用者的热情，从而形成我国区块链发展的良性循环。产业内动态值得跟踪关注。

8、看好区块链的哪些创业方向？区块链处于哪个阶段？

如果某些领域的信用成本很高或者缺乏信任，那就是有机会的，如跨国贸易金融领域，两个国家之间的融资、抵押等等；又如小蚁区块链，非常看好，它的口号是做证券市场的 Uber。

现在的证券市场有个很大的问题，很多资金集中在一级市场，二级市场门槛特别高，始终有个政府租值存在，而小蚁提供一个解决方案，把门槛降得很低，即利用这一套产品就可以发行数字资产，这些数字资产都是可以被交易的，只要有交易所愿意流通它，就可以运行起来。

其他的，如医疗的病例分享、审计领域、公证领域、物联网领域（物品的追溯、回溯）、供应链金融、保险（销售成 本过高）等等，都有创业的案例出来。

目前区块链处于第一个泡沫阶段，它太热了，但可能还没有处于顶端；国外的资金都是几十亿地往这个领域投，但国内的资金都没有动，因此还没有达到顶端，应该 是上升阶段。

区块链—基于底层去中心化的新信用机制

区块链专家陶荣祺表示，数字货币和区块链的发展带给我们“真实”感。我在区块链领域从业大概两三年， 目睹了类似地球生态中生物进化的过程，从无到有逐步进化。比特币从 2009 年创始到现在也就是 7 年的时间，在这 7 年时间，它一点点地成长了起来。我们把它看作 一个从无到有的货币也好、现象也好、状态也好，去观察它都是非常荣幸的。能够观察到一个系统、一个生命体，说得宽泛一点，一种状态是如何从无到有发展起来的， 这带给我的冲击是从无到有、完完全全、自下而上的。这样的成长是符合经济学原理的，**第一个含义就是往低成本的方向去走**；我理解经济学的第二个含义，**就是满足人们需要的，比特币和区块链这几年来的成长就是如此。**

我们现在看到的很多经济社会 状态，比如为什么要进行供给侧改革、共享经济，本质上就是因为满足人们需要的成 本太高。区块链也能看到这样的趋势，因为它是能够搭建人与人之间信任的一座桥梁。现在人与人之间的信任活动更多地基于国家政府、文化习俗的现行体系。文化习俗的积淀是很深的，没有问题，但国家机器是有缺陷的，这个问题在于经过考验的时间不足，毕竟国家机器仅成立了几十年的时间，可能还不够完善。

可以看出，文化习俗、 国家机器为我们建立起来的信用体系的成本目前偏高，尤其是国家机器，因为它强制需要很多制度、很多人（可能超过总人口 10%）来维持这个体系。同时，不管是哪一代人，劳务成本是差不多的，所以不管是哪个时代，10%的人来维持体系，其成本必然过高，更何况目前的信用体系还是不够好，比如春节联欢晚会要提出建立诚信社 会，本质原因还是社会不够诚信。

一种低成本的信用机制诞生，并慢慢地茁壮成长， 即区块链，必然会得到关注和推广。

区块链的信任来自于底层技术，即用历史信息换得现行的信任。现在我们去看 财务报表时会想财务报表是否提前被修改过，同时，现在的财务报表是横截面的。而 比特币区块链是 10 分钟建立一个区块，并盖好时间戳。

从密码学来说，一旦盖好时间戳，这个区块就没有办法破解。从创始到现在，每 10 分钟的时间戳包含这 10 分 钟全世界所有的交易信息，这意味着历史交易信息都在你的手里，并且无法篡改。

区块链带来的冲击就在于用时间换取人们的信任。类似地，如果政府运行时间越长，并且每次说的都能做到，民众的信任度也会增加。比特币的特点是，运行时间越久，篡改的难度越高，这是由它的设计机制保证的。

另外一个维度是区块链的交互。本质上说区块链是一个分布式的公开账簿，再往深层次理解，它实际是一个以太网的智能合约。中本聪在设计比特币的时候就是用智能合约的概念设计的，具体内容可以参考《区块链——新经济蓝图》的第二章。

合约的甲乙双方设计一个合约，合约内容描述某个条件或状态，这个条件一旦触发就执行； 传统合约的甲方乙方在条件触发时出现问题需要找国家机器、政府机关进行仲裁，这个在智能合约上是可以由区块链来做的。有人说区块链是去中心化脱媒，但实际上并没有完全脱掉，只是从国家机器、政府机关等转移到区块链本身来做。

当然，普通程序也可以设计很多合约出来，但问题在于代码是可以篡改的，因此内容无法得到完全的保证。**区块链则把所有内容都公开化，并且运用时间戳的概念使得所有内容不能被 篡改，因此智能合约是被强制执行的，从而可以把第三方仲裁、信任机构去掉，由区块链来执行。**

这实际上是从人的机构变成机器的机构，而机器的成本低于人类，所以 符合经济学原理。但是，我们刚才所讲的仍然是信任，并没有做到去信任。本来信 国家机构、政府机关、文化习俗的强制执行，现在转变成区块链、机器，就真的可以 相信吗？这**里有两个重要问题：第一，机器会取代人类吗；第二，机器会故障吗？**这些问题还有待讨论。

现在区块链有个概念叫做公开链、联盟链、私有链。公开链指，区块链的参与者是全世界所有的矿工，如比特币的公开链中，每个币址中有多少比特币完全公开，但币址指向于谁完全不知道，因此比特币是半匿名。

银行希望使用区块链但并不想将信息公开的话，就可以使用私有链。这种是受到控制的区块链，可以让区块链中有些信息公开，但有些信息不公开，这个开关可以自己设置。

虽然银行希望将区块链放在自 己的机房里来维护，但这与普通的数据库有一定区别。因为私有链的存在，几乎所有的金融机构都在研究区块链，特别是银行业基本每家都设有一个部门研究。

联盟链是指，区块链信息由多个人录入，而联盟中的对象是可以分享信息的（信息分享程度另 论），联盟以外的就无法获得信息，这类似于银联卡组织。**区块链解决了囚徒困境中的背叛选项，能够实现强制执行，相比于跨国之间信任度很弱的合作来说是进步的。**