【一文读懂比特币和区块链】区块链技术与应用

厦门大学计算机科学系 林子雨 博士/副教授

2020 年 1 月 2 日

【备注】本文由厦门大学信息学院计算机科学系林子雨老师编写，内容素材全部来自网络，林子雨老师对网络大量资料进行搜集整理后编写了本文。本文可以作为林子雨编著《大数据导论（通识课版）》教材（官网：http://dblab.xmu.edu.cn/post/bigdataintroduction/）的配套教学内容。本文配套的讲义 PPT，请到《大数据导论（通识课版）》教材官网下载。

【引言】区块链是继云计算、大数据、物联网和人工智能之后的 IT 领域又一大热门技术。区块链蕴含着巨大的变革潜力，有望成为数字经济信息基础设施的重要组件，正在改变诸多行业的发展图景。继区块链技术列入“十三五”规划后，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习，区块链的国家科技战略地位再次提升，迎来发展机遇期。本文将与大家分享比特币的发展历史、区块链的概念与技术原理以及区块链的典型应用场景。

一、 疯狂的比特币

1、比特币的诞生

一切的故事，要从比特币的诞生开始。

2008 年 10 月 31 日，中本聪向一个密码学邮件列表的所有成员发送了一个电子邮件，标题为“比特币：点对点电子现金论文”。在邮件中，他附上了比特币白皮书的链接，论文题为“比特币：一个点对点电子现金系统”（Bitcoin: A Peer-to-Peer Electronic Cash System）。

中本聪在 2008 年发表的这篇论文可能是互联网发展史上最重要的论文之一，其他重要论文包括：利克里德写的开启互联网前身阿帕网的“计算机作为一种通信设备”（1968 年）、蒂姆·伯纳斯-李写的万维网协议（WWW）建议书“信息管理：一个建议”（1989 年）、谷歌联合创始人谢尔盖·布林与拉里·佩奇写的搜索引擎论文（1998 年）等。

2009 年 1 月 3 日，在位于芬兰赫尔辛基的服务器上，至今匿名的神秘技术极客中本聪生成了第一个比特币区块，即所谓的比特币“创世区块”。

在创世区块的备注中，中本聪写入了当天英国《泰晤士报》的头版头条标题：“*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*”（*《泰晤士报》，2009 年 1 月 3 日，财政大臣站在第二次救助银行的边缘*），

这样做，他记录了比特币系统启动和创世区块生成的时刻，又借这句话表达了对当时全球金融体系的暗讽。2009 年年初，全球金融体系刚经历了 2008 年金融危机的冲击，看起来摇摇欲坠。

在生成创世区块时，按自己设定的规则，中本聪获得了 50 个比特币奖励，这是最早的 50 个比特币。从创始区块开始，在比特币的账本上每 10 分钟就有新的数据区块被增加上去，新的比特币被凭空发行出来。比特币的去中心网络开始运转，扩展到现在的由数万个节点组成的全球网络。

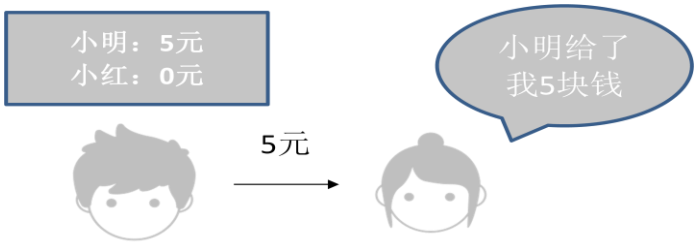
2010 年，他逐渐淡出并将项目移交给比特币社区的其他成员。中本聪据信持有约一百万个比特币。这些比特币在 2013 年底时的价值超过十亿美元。

从发表论文以来，中本聪的真实身份长期不为外界所知，维基解密创始人朱利安·阿桑奇（Julian Assange）宣称中本聪是一位密码朋克（Cypherpunk）（密码朋克提倡信仰使用强加密算法将能够使个体保持安全的私人性，他们反对任何政府规则的密码系统。他们可能容许罪犯和恐怖分子来开发和使用强加密系统，但接受为个人隐私付出风险）。另外，有人称“中本聪是一名无政府主义者，他的初衷并不希望数字加密货币被某国政府或中央银行控制，而是希望其成为全球自由流动、不受政府监管和控制的货币。”

在比特币的创世时刻，它的三个组成部分都出现了，即加密数字货币（cryptocurrency）、分布式账本（distributed ledger）、去中心网络（decentralized network）。

2、为什么要创造比特币

那么，中本聪为什么要创建比特币呢？这个就要从现实世界中的转账说起。比如，在现实世界中，小明要给小红 5 元钱。



第一种方式是，小明可以把现金纸币 5 元钱给小红，不需要经过诸如银行、支付机构、见证人等中介机构。但是，随着互联网的普及，电子支付越来越流行，人们越来越少使用纸币。在电子支付中，就会有一个权威中介机构（比如银行）负责记录这笔转账交易。

但是，记账权掌握在一个中心化的中介机构手中，不仅需要交纳中介手续费，还可能存在中介系统瘫痪、中介违约、中介欺瞒、甚至是中介耍赖等风险。例如，2017 年 4 月，民生银行 30 亿假理财事件暴露，系一支行行长伪造保本保息理财产品所致，超过 150 名投资者被套。再比如，2013 年 3 月，塞浦路斯为获得救助，对银行储户进行一次性征税约 58 亿欧元，向不低于 10 万欧元的存款一次性征税 9.9%，向低于 10 万欧元的一次性征税 6.75%。

另外，传统的货币的发行权掌握在国家手中，存在着货币滥发的风险。例如，元朝自 1271 年建立后，依然四处征战，消耗大量的钱财和粮食，为了财政问题，长期滥发货币，造成严重通货膨胀，多数百姓生活在水生火热中，导致流民四起，国家大乱，1368 年，不可一世的元朝成了只有 97 年寿命的短命鬼，走向了灭亡。再比如，1980 年津巴布韦独立，后因土改失败，经济崩溃，政府入不敷出，开始印钞；2001 年时 100 津巴布韦币可兑换约 1 美元；2009 年 1 月，津央行发行 100 万亿面值新津元加速货币崩溃，最终津元被废弃，改用“美元化”货币政策。2017 年津巴布韦发生政变，总统穆加贝被赶下台。

在数字世界中，如何创建一个无须中介或者说去中心化的数字现金，一直是一个难题。由于数字文件是可复制的，复制出来的电子文件是一模一样的，因而在数字世界中，我们不能简单地用一个数字文件作为代表价值的事物。由于数字文件可以完美复制，如果没有一个中心化数据库做记录，那如何避免一个人把一笔钱花两次？这就是所谓的双重支付或双花问题（double spending）。在比特币出现之前，我们熟悉的主要电子现金系统（如 PayPal、支付宝等）都是依靠中心化数据库来避免双花问题，这些可信第三方中介不可或缺。但是，上面我们已经阐述过，存在中介会带来各种问题。

在去中介或去中心化的电子现金这条路径上，有很多技术极客一直在做着各种尝试，只是一直未能获得最终的成功。

到了 2008 年，中本聪借鉴和综合前人的成果，特别是现在常被统称为密码朋克（cypherpunk）的群体的成果，改进之前各类中心化和去中心化的电子现金，加上自己的独特创新，创造了比特币这个点对点电子现金系统，在无须中介的情况下解决了双花问题。

特别地，比特币这个电子现金系统是同时去中介化和去中心化的：个人与个人之间的电子现金无须可信第三方中介的介入，这是去中介化。这个电子现金的货币发行也不需要一个中心化机构，而是由代码与社区共识完成，这是去中心化。

最初，比特币这个用以表示价值的电子现金并没有价格。比特币系统只是在逻辑上可行的系统，是解决了一个难题的技术玩具。2010 年 5 月 22 日，在一个网络论坛上，有一个程序员用 1 万枚比特币换了两张棒约翰比萨的代金券，比特币第一次有了一个公允价格：1 万枚比特币价格为 25 美元。为了纪念这一天，每年的 5 月 22 日变成了区块链世界的一个节日——比特币比萨节。

此后，比特币虽然从来都不是货币，但逐渐地有了价值与价格。比特币的价格在自由市场交易中被确定，又持续、反复地大幅波动。但是，不管是从早期的 1132 美元跌掉一半，还是在 2017 年年底快速上涨到接近 2 万美元，又在几个月内跌到只有三分之一，比特币系统和它底层的区块链技术都保持稳定。

中本聪设计和编码实现的比特币电子现金系统至今已运转近十年。比特币系统已经从一个技术玩具变成一个运转得近乎完美的系统，并且看起来还将长期稳定地运转下去。

3、比特币的传奇故事

在比特币的江湖上，流传着许多动人的故事。

【故事一】一个社区网站的站主凭借 3000 枚比特币发家致富

2009 年，20 多岁的单身男青年小伟，热衷于搜集各种小电影资源，为此他还建了一个社区，还可以花钱成为社区 VIP，看到更多好片。

在社区里有一位程序猿大哥，表示想花 3000 个比特币买 VIP 的资格。

“啊？彼特毕？彼特毕是啥子？我这里的 VIP 收费一年要 300 块呢！”小伟根本没想理他。

可是，程序员大哥哪里是吃素的，架不住大哥的软磨硬泡，后面小伟只能答应了。程序猿大哥也很实在，把 3000 个比特币打给了小伟，还教了他怎么挖矿。

小伟虽然是一脸懵懂，但是也被动地接受着，不过这事他很快就忘了。

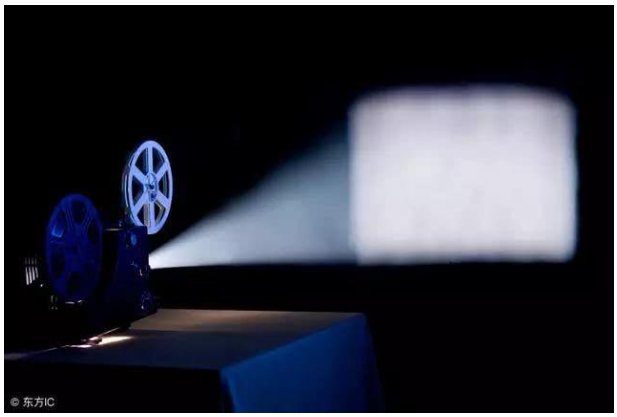
经历了生活的种种艰难，8 年后的小伟依旧兜比脸还干净。

在偶然间，听到周围的人说起比特币，小伟也猛然想起，8 年前那个跟他买 VIP 的程序猿大哥，于是他翻箱倒柜地把密钥找了出来。

当时，一个比特币 4 万元人民币。

穷了 30 多年的小伟，在深圳买了十套房，目前正在找媳妇，他也不用再靠小电影活着了。

可他还是很想念当年那个程序猿大哥。



【故事二】48 万哥的故事

这个故事的主人公，江湖上都称他为“48 万哥”。

2014 年 1 月 28 日，“48 万哥”在比特币吧开了一个帖，称将自己存了七八年的 48 万元房款，用来买了 100 个比特币。他志得意满地说：“期待大赚一番，买房直接全款，运气好的话把车也换了。”

随后，网友们见证了他每日心情的起起伏伏：

“跌了 10 块，少了 1000 块。”

“小涨 40 元，赚了 4000 块。”

“短期内不会卖出，除非翻倍。”（有人说他“做梦！”）

谁想，不久负面消息频出，国家不承认比特币的价值、平台关闭、大佬跑路等新闻一个接一个。

比特币从 8000 多一下子跌到了 2000 多，“48 万哥”在贴吧里被疯狂嘲笑。

2015 年 1 月，“48 万哥”变成了“6 万哥”。

2016 年 1 月，将近两年过去，比特币 3000 元左右，他再也坚持不住了，割肉买房了。

从此之后，“48 万哥”再也没有出现过，但人们对他的关注却从未停止，跟贴已有一万多，还有人把他写进了小说里。

【故事三】英国小伙子要集资挖开垃圾填埋场

为了 7500 枚比特币，他众筹 740 万英镑，请求政府让他挖开垃圾填埋场。

这个倒霉蛋，就是英国小伙子豪威尔。

2009 年 2 月，豪威尔用自己的戴尔电脑挖矿。几年下来，豪威尔存下了 7500 枚比特币。

因为比特币的价值涨幅不大，2013 年，他停止了挖矿，并把之前挖矿的电脑卖了，只留下硬盘。

2013 年夏天，一次大扫除中，豪威尔无意中将这块硬盘丢进了垃圾箱。

后来，比特币价格飞涨。2017 年 12 月，后悔不迭的豪威尔找来了几位“股东”，筹资了 740 万英镑给政府，要求挖开垃圾填埋场。

尽管他请求再三，但政府还是拒绝了。理由是挖开垃圾填埋场可能伴随严重的环境污染，还可能引爆危险气体。

豪威尔气坏了，却也无可奈何。

直到如今，那 7500 枚比特币，还在英国的一个垃圾场下面沉睡着。

4、比特币与传统货币的区别

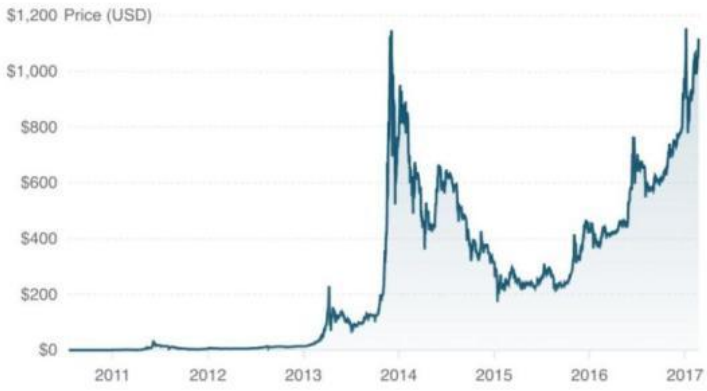
那么，比特币和国家发行的货币，有什么区别呢？具体请看下表。

对比		
由央行控制	稀缺性	总量只有2100万个
国家	信用背书	不可更改的程序、参与者的共识
较高，需要第三方清算机构	交易成本	较低，点对点，无需中介
一般	流动性	极高、无国界
纸、油墨	铸币成本	电费、矿机（1万/BTC）

5、比特币的暴涨暴跌

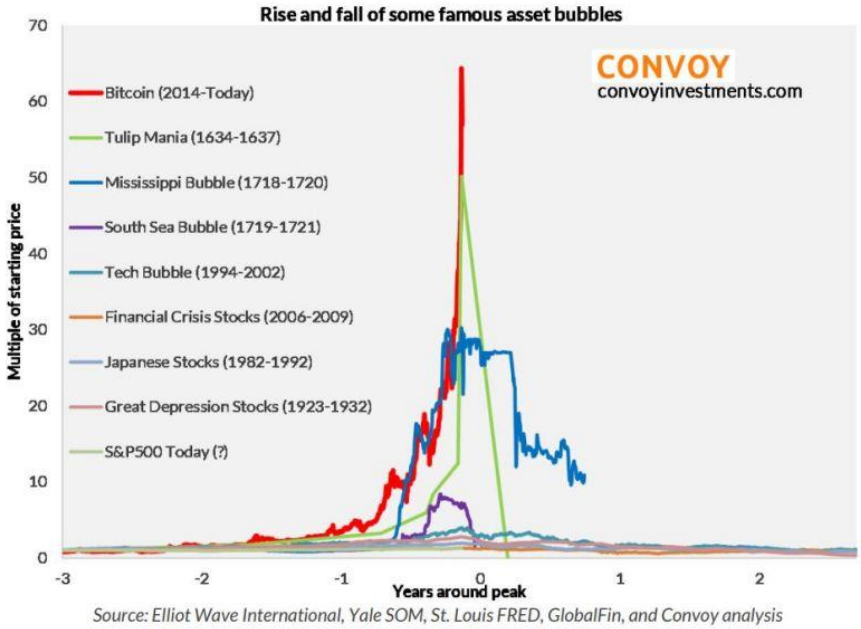
如果要谈到近 10 年最成功的风险投资，那一定是比特币了，10 年间收益率累计收益 1300 万倍，这样的收益率，我想就算是马云爸爸也望尘莫及了。

“郁金香泡沫”是人类历史上第一次有记载的金融泡沫。16 世纪中期，郁金香从土耳其被引入西欧，不久，人们开始对这种植物产生了狂热。四百年后，比特币“借尸还魂”出现在世界各地，但“郁金香泡沫”与之相比，可算是小巫见大巫。2009 年比特币刚出现的时候 1 美元可以买到 1300 枚比特币，而今日比特币的价格为 1.35 万美元，比特币在仅仅 8 年时间里价格就暴增了 1700 多万倍！然而更可怕的是，比特币数量有限，只有 2100 万个，并且全世界 86.66%的比特币掌握在 0.57%的人手里，其市场极易被操纵，造成比特币价格暴涨或暴跌。



2017 年底，比特币价格一度突破 2 万美元，站上了一个令人晕眩的历史高峰。

要知道在 2010 年，一份价值 25 美元的披萨就花掉了买主 1 万枚比特币，相当于一枚比特币价值 0.25 美分。七年时间身价暴涨 400 万倍，使得比特币超过荷兰“郁金香狂热”和英国“南海公司骗局”，成为人类历史上最大的一次资产泡沫。

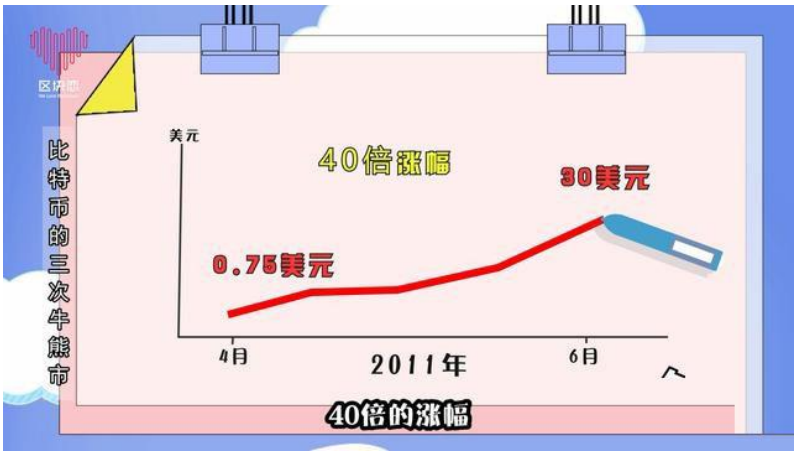


Source: Elliot Wave International, Yale SOM, St. Louis FRED, GlobalFin, and Convoy analysis

第一次暴涨暴跌：2011 年到 2013 年

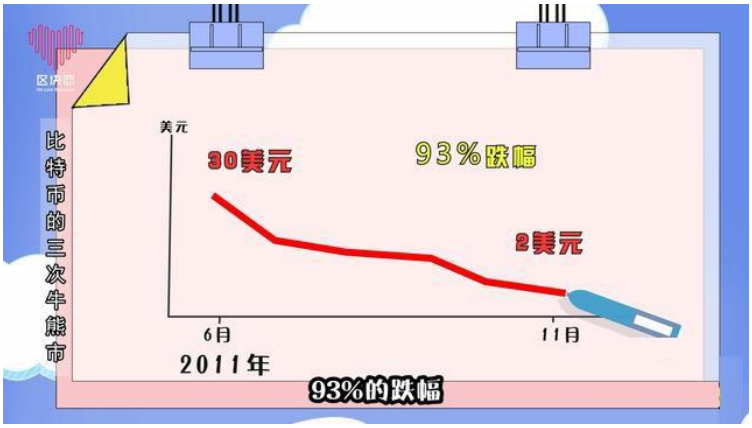
在 2011 年的 4 月到 6 月，仅仅两个月，比特币从 0.75 美金一下子飙到 30 美金，**40 倍的涨幅，细算下来，相比于比特币诞生时的 0.0076 美金，涨了 4 万倍啊，太吓人了。**

那为什么突然会从 0.75 涨到 30 美金？原来是因为比特币与英镑兑换交易平台在那两个月上线了。然后美国一些主流报刊都开始报道比特币了，消息一出，全球投资者简直是趋之若鹜的加入炒币行列了。



2011 年 6 月之后，一直到 11 月，比特币就从 30 美金跌到了 2 美金，涨起来吓人，跌下来更吓人，93%的跌幅，估计刚加进来的小白菜们啊，胆子都要吓破了。

这么大幅度的下跌，根本原因，可能与 2011 年 6 月份全球最大的比特币交易平台门头沟（Mt.Gox）被黑客攻击有关。涨了那么多，黑客当然不会放过了。



第二次暴涨暴跌：2013 年到 2015 年

2013 年 1 月到 12 月，11 个月内，比特币从 13 美金，涨到了 1147 美金，88 倍的涨幅。**与诞生价相比，涨超 100 万倍**。这个时间段，也发生过黑客攻击，引发过价格回调。不过依然是牛气哄哄的保持了千元美金的价格。

能涨这么多的原因啊，主要是因为塞浦路斯的债务危机，引发了传统金融机构的信任危机。然后，13 年下半年，欧洲的部分国家出台了对比特币有好处的政策，这下好了，知道比特币的人越来越多。投机者自然不肯放过这个机会。

只要这些投机者一出现我就知道没什么好事，这不，好不容易涨起来的，又暴跌了。

2013 年 12 月到 2015 年的 1 月，一年多，比特币又从 1166 美金，跌回了 170 美金，85%的跌幅。

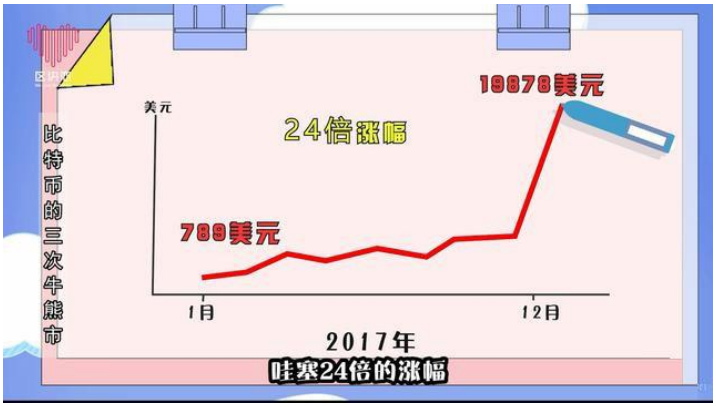
暴跌的原因，估计与 13 年 12 月中央五部委发布的《关于防范比特币风险的通知》有关。因为通知发布后，比特币在 83 天内，暴跌 92.5%。那个时候数字货币在人们的认知范围内也没现在那么大影响力。所以防范是没错的。

第三次的暴涨暴跌：2017 年 1 月到 2018 年 9 月

这个时期是比特币最重要的两年了，因为比特币在 2017 年的一年间，就从 789 美金，**涨到了 19878 美金。24 倍涨幅。与比特币的诞生价相比，涨了 2000 万倍**。

原因：这一年，比特币的底层技术区块链技术强势崛起，带动了比特币价值飙升。同时以太坊的 ICO 的爆发，引发了比特币的暴涨。

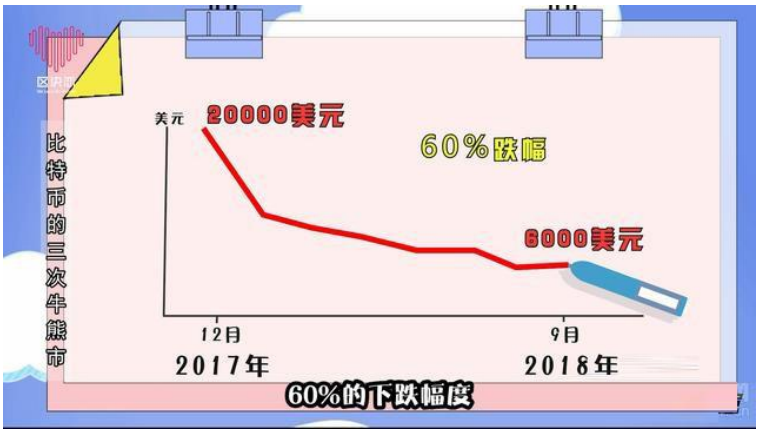
两万美金啊，让很多人一夜之间，从屌丝变土豪了。这下子不光是投机者，比特币这个东西，地球人都知道了，肯定引来了更多的吸血鬼，也引来了不少国家带着杀气的目光。



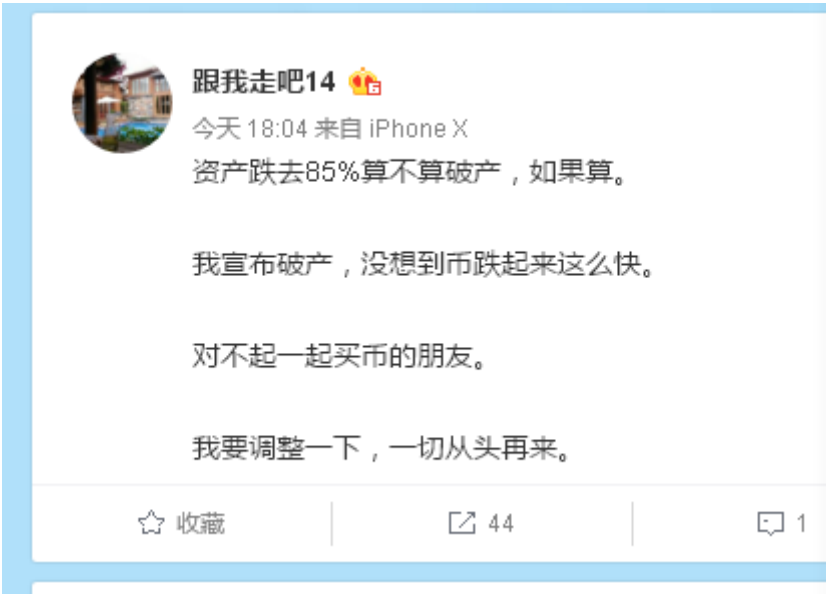
这不，估计比特币史上少见的漫长熊市就要来了。

从 2017 年 12 月到现在，比特币一直处于熊市，从两万美金跌倒了 6000 多美金。60%的跌幅，让很多人开始怀疑人生。

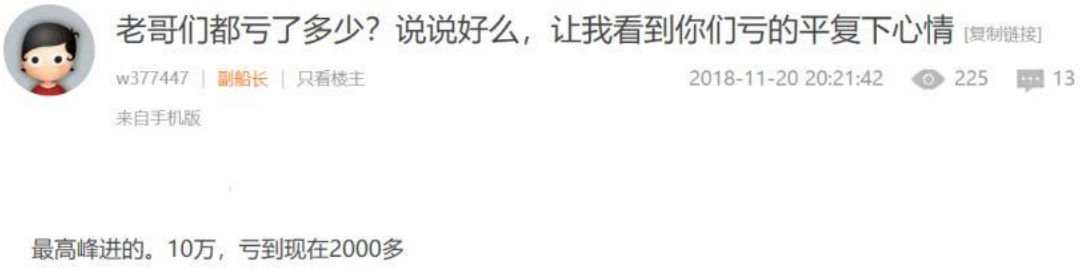
这次的下跌有很多原因，全球监管变得严了，交易所老被攻击，投机者的们脆弱的小心脏不堪重压，都有关系。



6、投资比特币的喜与悲



有网友发帖表示，自己在币价最高峰时投入的 10 万元，现在只剩下 2000 多元，相当于亏掉了 98%的本金。在比特币“老大哥”颓势影响下，其他较小加密货币跌幅更惨重。据记者不完全统计，在 2479 个加密货币中，价格在人民币一毛钱以下的有 1400 个，一分钱以下的有 611 个。很多“山寨币”、“空气币”价格接近归零，投资者血本无归。



有一些人从比特币的“潮起潮落”中，找到了发财的机会。这就是比特币世界中的“搬砖”客。所谓“搬砖”就是从一家报价相对较低的交易平台买进比特币然后到报价较高的平台出售的过程。2013 年 4 月，当时还在美国伯克利留学的中国学生袁浩瀚和朋友悟空在收集比特币价格数据的时候发现，在不同交易所之间比特币存在非常大的差价，尤其在不同国

家之间，那时中美比特币差价长期维持在 30%到 50%之间。

7、比特币财富排行榜

比特币发展到今天，拥有比特币最多的人是谁？比特币持有人的前十名如下：

- 第一名，98 万枚比特币，持有人中本聪(Satoshi Nakamoto，比特币创造者)；
- 第二名，40 万比特币，持有人 HD Moore(Metasploit 项目创始人)；
- 第三名，40 万枚比特币，持有人 Dustin D. Trammell(网络安全研究者，建立了在线社区如 ExploitHub)；
- 第四名，40 万枚比特币， 持有人 Tod Beardsley(Metasploit 项目框架技术负责人)；
- 第五名，35 万枚比特币，持有人 Ross Ulbricht (丝绸之路的创始人和管理员)；
- 第六名，30 万枚比特币，持有人 Roger Ver (人称比特币耶稣)；
- 第七名，30 万枚比特币，持有人“knightmb”(身份未知)；
- 第八名，20 万枚比特币，持有人 Mark Karpeles(法胖，Mt.Gox 平台老板，现在拥有多少币未知..)；
- 第九名，18.3 万枚比特币，持有人”Loaded”(身份未知)；
- 第十名，17.4 万枚比特币，持有人 FBI，美国政府。

在榜单中排名第一的中本聪的特别，不仅仅在于他是个天才。他的比特币钱包有一百万个比特币，以今天的价格算价值上千亿。

【丝绸之路】

这里还要讲讲榜单中排名第五的 Ross Ulbricht (丝绸之路的创始人和管理员)。2011 年，在物理和材料化学方面颇有建树的乌布利希凭借自学的编程知识创建了暗网“丝绸之路”。所谓暗网指的是那些无法使用普通的搜索引擎访问，通过洋葱路由层层加密形成的层叠网络，十分隐秘难以追踪。

在网络搭建完成之后，乌布利希成为了进驻的第一个商家，他将自己和女朋友种的致幻蘑菇放在上面挂牌出售，交易方式明确规定需要使用匿名性极强的比特币，很快他们收获了第一笔资金。随后，便不断有毒贩慕名而来，不到两个月丝绸之路的用户数量就超过了 100 万，商品种类超过上万种，其中有七成还是毒品，除此之外暗网上还出售假钞、枪支弹药、假护照驾驶证和盗用的信用卡信息。

丝绸之路管理非常到位，只要发现有人卖假毒品，已经查实马上封号。于是有人评价丝绸之路：“就像 Uber 改造了出租车行业一样，丝绸之路让毒品交易变得安全、有趣和友善。”

各色人等在这个网络空间里进行非法交易，而作为管理员的乌布利希每天忙碌着为卖家提供各种手册，教他们如何密封毒品，安全交易躲避追踪。当然，好处也不少。通过收取交易中的 8%~15%左右的手续费，他在两年时间内狂赚 12 亿美元，折合 77 亿人民币。

但丝绸之路对于一般的警察来说，简直是个迷宫。使用去中心化的虚拟货币让买卖很难被追踪。暗网又用了“洋葱路由”技术， 像剥洋葱一样，一层又一层代理连接，追查起来

非常困难。就算费尽九牛二虎之力，也不见得有什么收获。

2012 年 4 月，乌布利希收到一个价值 10 亿美元的交易请求。对面是一个来自多米尼亚共和国的毒品走私犯。

这个大毒枭的出现让乌布利希觉得还蛮有意思的，毕竟有大佬认可自己。他问对方有没有什么具体的投资方案。结果对方直接叫价 10 亿美元，并给出了实施方案，但乌布利希果断拒绝了对方。但他并不知道，对方其实是传奇卧底特工卡尔·佛斯（ Carl Force），危险正在靠近 。最终，乌布利希被抓获判刑。

【比特币耶稣】

在榜单中排名第六的是人称比特币耶稣的 Roger Ver（罗杰·维尔）。耶稣是基督教里的救世主，根据《圣经》记载，他将在世界穷尽之时降临，给“善”带来最后的胜利。而在比特币的世界里，也有这样一位救世主：他对比特币的布道和支持可以说是呕心沥血，曾救比特币于危难之际。他是第一个比特币天使投资人，也是 Bitcoin.com 的 CEO，据说他最多时持有 30 万颗比特币。这个人就是被誉为比特币耶稣的 Roger Ver（罗杰·维尔）。

罗杰生于硅谷，家境富裕，从小就展现出从商的天赋。初中时靠倒卖糖果，每周为自己赚得 50 美金。高中时的他开始阅读大量的经济学书籍，并对**自由经济**有自己独到的理解。大一时，他创办了自己的公司——Memorydealers，并随后退学。

2000 年，年仅 21 岁的他就以自由党候选人的身份参加州议会的选举。不幸的是，他被其他政党成员举报在网上无证卖炸药，后来他因此被判刑 10 个月。

牢狱之灾没有击垮年轻的罗杰，出狱后他一心从商，并将自己的 Memorydealers 转型为电子设备公司，后来公司业务拓展到日本，罗杰也成为了小有名气的企业家，这也为他后来成为比特币天使投资人奠定了经济基础。

2010 年底，罗杰像往常一样听着自己最爱的广播节目——Free Talk Live，突然一个陌生的词语让他产生了好奇——Bitcoin。但当时的比特币还过于冷漠，所以这份好奇心也没有持续多久。

直到次年的 3 月，比特币的价格陡然突破 1 美元，这个消息让罗杰再也坐不住了。经过对比特币的深入研究，他买下了自己人生中第一个比特币。

后来他发现对于一个经济自由主义者来说，比特币实在太完美了，它的意义甚至超过互联网。他实在按捺不住自己激动的心情，以至于**因兴奋过度而病倒住院**。

出院后，罗杰做的第一件事情就是让自己的公司 Memorydealers 接受比特币支付，他还为此特意做了一个广告牌安装在硅谷的 Lawrence 高速公路旁。

罗杰不仅自己大量购买比特币，还经常在广播电台打广告。**自此，他正式开启了比特币的布道生涯，并为自己赢得了比特币耶稣的称号**。

2011 年 6 月，当时最具影响力的比特币交易所 MT.GOX（门头沟）被黑客入侵，造成数千比特币的损失，以及大量用户信息的泄露。正当交易所一筹莫展之际，比特币耶稣罗杰如及时雨一般出现。

要知道罗杰的第一个比特币就是在这里买的。

他深知如果 MT.GOX 倒下，一定会对比特币产生重大打击。为了保护和支持比特币的发展，罗杰毅然决然的躺了这趟浑水。他请朋友一起来日本帮助 MT.GOX 进行危机公关，甚至是修复 BUG。

不过虽然交易所的危机解除，并且网站也重新开张，但是比特币的声誉却依然受到了严重影响。2011 年 7 月比特币价格从 31 美元暴跌到 2 美元，越来越多的人开始指责比特币就是一场骗局。

比特币耶稣罗杰再次挺身而出，并下注 1 万美元打赌称：“比特币的涨幅会远超黄金、白银甚至是美国股市，并且两年内它的涨幅会超过 100 倍。”

不过这次罗杰赌输了，因为比特币完成 100 倍涨幅的时间是两年零两个月。

虽然比特币大跌，但是随后的纽约比特币大会还是如期举行了。曾经只能在网络上交流的币圈人终于在现实中碰面。这次大会上，罗杰认知了比特因斯坦的创始人查理·西仁，并且一下就投了他 12 万美金。不仅如此，他还推荐自己的朋友帮助比特因斯坦的发展，后来这家公司的成功也标志着第一批比特比企业的兴起。

2012 年，比特币开始企稳，后来涨幅也超过了美国股市，罗杰也开始投资更多的比特币公司。在这些年的发展中，他投资的公司，有些已经退出历史舞台，而有些则赫赫有名。

在罗杰看来，相比投资回报而言，**最重要的是支持那些对比特币有坚定信念，对世界有更多美好憧憬的创业者**。这就是比特币耶稣——罗杰·维尔。

【中国比特币首富】

这里还要谈一谈中国的比特币首富——李笑来。李笑来曾经是新东方的一名英语教师。从新东方辞职后，李笑来创办了多家科技公司和教育公司。他还成立了一家投资公司，因为他投资了比特币。李小来还开设了一门以互联网财富为主题的付费课程。这门课的观众人数很多。每年，李笑来通过这种方式赚取数千万美元。据有关人士透露，李笑来现在身价数十亿美元，我相信他将来的身价会更高。

8、疯狂追逐比特币的国家——韩国

说到对比特币最狂热的国家，那就不得不提到韩国。韩国在比特币方面尤其活跃。韩国是世界上三大交易所的所在地，占全球比特币交易总量的 20%。据估计，韩国有 200 万人拥有比特币和其他数字货币。在韩国，比特币的交易量已经超过股票市场。

还有报道称，投资虚拟货币的韩国人中，超过 80%获利，约 20%获得了平均 425%的投资回报。

《首尔新闻》采访的一位应届生就在投资比特币后暂停了学业。他说，与其继续在找工作的路上屡战屡败，倒不如专心投资虚拟货币，一举摆脱就业大军。他感叹称，普通的公司员工就算十年不吃不喝，也买不起首尔的一套房，所以他就算找到工作也改变不了自己灰暗的未来。

另一位投资虚拟币的上班族也时常在工作中翻看手机。他说有一位朋友的同事靠虚拟货币赚了大钱，换了辆车，甚至连在首尔江南区买房的钱都准备好了。周边的朋友们也通过投资虚拟货币赚到了数百万韩元到数千万韩元不等的资金。

“能改变人生的机会似乎也就这么一次了。”

《首尔新闻》报道称，目前韩国对虚拟货币的管理还很不规范，比如人们无需为虚拟货币的收入纳税。虽然韩政府已经加大了对该类资产的监管、核查力度，但韩国人对虚拟货币的热情却只增不减。报道认为，各种投资几万韩元却获利几十亿的“鸡汤故事”起到了煽风点火的作用。

对此，韩国庆北大学社会学系卢镇哲教授表示：“年轻一代人熟悉网络，不会排斥虚拟货币，反而会像游戏一样乐在其中。”他还称，跟股票相比，虚拟货币的波动更大，相当于是孤注一掷的赌博，会对日常生活造成妨碍，必须制定相关的规则。

（上图韩国比特币贸易公司“Coinplug”制造的比特币专用取款机）

9、比特币为什么会上涨

现在，需要讨论一个问题，比特币为什么涨？

其中一种声音是：“为什么比特币会涨呢？因为国际政治经济的周期，5000 年来所有法币无一例外全部失败，5000 年来黄金持久不衰，5000 年来第一次有了安全数字技术可以代替黄金功能。所以比特币的使命就是历史使命，是先超越黄金，再代替全球储备货币美元，无非是时间问题。”

实际上，比特币之所以会涨价，主要包括以下几个原因：

（1）炒作。前期，肯定没有人觉得比特币、数字货币是可以为实体服务的。但是为了让这新的市场繁荣起来，那么肯定有一部分人开始炒作，拉动人气。要知道比特币刚刚开始的时候，才几分美元，有人用 20000 个比特币吃了一个披萨以后，才让人看到比特币的实体应用功能，接着比特币才被炒的火起来。炒作，是比特币上涨的原因之一。中期，随着比特币长时间的炒作，那么有部分人也意识到了它的价值，有团队也就开始接着发展比特币技术。这样一来，比特币随着时间的推移，技术完善，数量稀少，炒作厉害，受到各路大神追捧，价格也就慢慢的上去了。后期，落地应用，推广，实体交易，在把比特币的地位摆放开了以后，人们就觉得比特币上涨应该理所当然了。

（2）交易不受限制（绕过外汇管制，洗钱）。

（3）数量稀少。比特币总量是不变的，只有 2100 万枚，但是用户数在不断增加，因此，物以稀为贵，比特币就会不断升值。

（4）被赋予投资品的意义。

（5）落地应用（星巴克、沃尔玛支持比特币支付）。

（6）去中心化（一种避险产品，功能堪比黄金）。比特币是去中心化的，没有掌握在一个人或者一个组织手里，是不受控制的。这样就会让很多人觉得安全。从而使它变成一种避险产品，功能堪比黄金，甚至在某种情况下，它比黄金还要方便。因为比特币不占地方，也不会被人打劫。但是黄金就不一样，笨重还占地方。安全性也不好。总之而言，比特币跟黄金比，现在可能比不上，但是不代表以后比不上，5 年肯定会超过黄金的价值。这没有什么可以争议的。因为比特币的属性决定了它的价值。

二、区块链原理

区块链（blockchain），这个中文翻译最早是 2013 年由世纪互联数据中心的创始人、董事长陈升提出的。区块链是比特币背后的技术，比特币和区块链是同时诞生的。比特币背后的技术被单独剥离出来，称为区块链。

1、从记账开始讲起

那么，什么是区块链呢？这里需要从记账开始讲起。

货币最重要的行为就是交易，交易会产生记录，就需要记账。比如，如下图所示，这个账本就记录了很多条交易。比如，编号为 395 的记录，表示张三给李四转账了 10 元钱，编号为 396 的记录，表示张三给王五转了 50 元钱，编号为 398 的记录，表示央行发行了 1000 元货币。

从数据的结构来说，每次转账其实就是一条数据记录，我们把这种方式叫做记账方式，就是记了一笔我转给她钱的账，这个记账叫**中心式记账**。法币是由我们信任的中心化机构（政府、银行）记账。几乎所有的银行都是用中心化记账的方式维护巨大的数据库，这个数据库保留我们所有钱的记录。

中心化记账有很多的好处，数据是唯一的，不容易出错。你如果足够信任它的话，转账效率特别高，在同一个数据库里一转就过去了，瞬间就转完了。

但是我们需要意识到，**中心化记账从金融角度来说有两个潜在的问题：**

第一，中心化的机构，真的可信吗？银行真的可信吗？你说银行不可信，还有谁可信？但确实银行有可能会出现问题，比如说大家可能从新闻报道上看到某某银行某某支行的行长通过交易漏洞，把钱挪出来，自己认为炒股可以赚了再放回去，结果赔了，亏空了，他就跑了。

第二个安全隐患是什么呢？银行建立中央化数据库，比如说中央化数据库在上海，一不小心出了很大的问题，整个数据库突然没了，硬盘坏掉了，怎么办？你说没关系，我们在新疆还有一个备份数据库，假设一颗原子弹也落在新疆，这两个地方都没了。理论上这个概率非常小，但并不是说完全没有可能。

而且，之前我们也说过，我们的信任往往会被辜负，可能会存在中介系统瘫痪、中介违约、中介欺瞒、甚至是中介耍赖等风险。

为了避免以上问题，是否有一种货币可以不用中心化机构来记账，这也是比特币发行的初衷。

2、比特币要解决的第一个问题：防篡改

不由传统的“可信”的中介机构记账，那么谁来记账？

怎样保证新的记账者不会篡改交易记录呢？

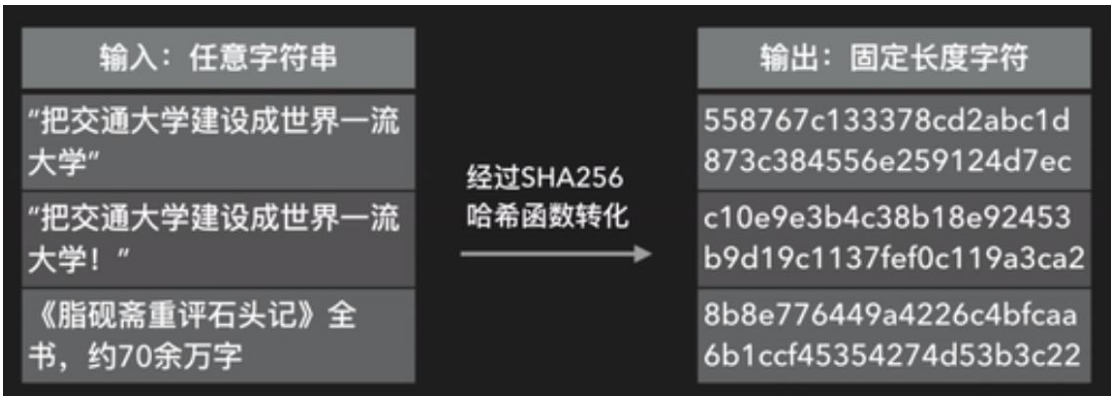
黑客攻击篡改交易记录怎么办？

这就是比特币要解决的第一个问题：防篡改。

为了实现“防篡改”，就需要引入哈希函数。哈希函数的作用是将任意长度的字符串，转变成固定长度的输出（比如 256 位），输出的值就被称为哈希值。哈希函数有很多，比特币使用的是 SHA256。哈希函数必须满足一个要求，就是计算过程不能太复杂，用现代计算

机去计算，应该可以很快得到结果。

比如，下图中，输入字符串是“把交通大学建设成为世界一流大学”，经过哈希函数转换以后，输出是“5587……d7ec”。当输入字符串是“把交通大学建设成为世界一流大学！”，经过哈希函数转换以后，输出是“c10e……3ca2”。可以看出，只要输入字符串发生微小变化，哈希函数的输出就会完全不同。



哈希函数有两个非常重要的特性：

（1）第一个特性：很难找到两个不同的 x 和 y，使得 h(x)=h(y)，也就是说，两个不同的输入，会有不同的输出；

（2）第二个特性：根据已知的输出，很难找到对应的输入。

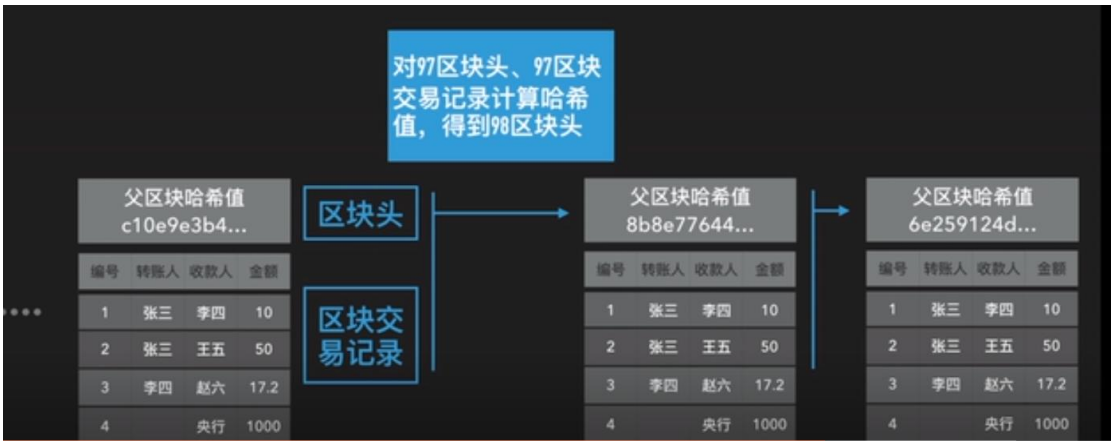
我们来看一下第一个特性。输入字符串是一个任意长度的字符串，是一个无限空间。而哈希函数的输出是固定长度的字符串，是一个有限的空间。从无限空间映射到有限空间，肯定存在多对一的情况，所以，肯定会存在两个不同输入对应于同一个输出值。也就是说，肯定存在两个不同的 x 和 y，使得 h(x)=h(y)。虽然这种情况在理论上是存在的，但是，实际上不知道用什么方法可以找到。因为，这里面没有任何规律可言，需要用计算机把所有可能的字符串都遍历一遍，但是，即使用目前最强大的超级计算机去尝试，也几乎要花费无穷无尽的时间，才能找到这样一个字符串。现在计算机找不到，那么，将来计算机发展了，是不是很容易可以找到呢？没有问题的，如果计算机变得强大了，那我只要把哈希函数输出值的长度变得更大即可。

了解了哈希函数以后，现在就来看一下什么是区块链。

刚才讲过，所有的交易记录都被记录在一个账本中。这个账本非常大，于是，我们可以把这个大账本进行切分，切分成很多个区块进行存储，每个区块记录一段时间（比如 10 分钟）内的交易，区块与区块之间就会形成继承关系。以下图为例，区块 1 是区块 2 的父区块，区块 2 是区块 3 的父区块，区块 3 是区块 4 的父区块，依此类推。每个区块内记录的交易的条数可能是不同的。10 分钟生成一个区块。如果 10 分钟内发生的交易次数较多，则这个区块记录的交易条数就较多。

可以把一个个区块，理解成一个个 EXCEL 文件。我们有台电脑，这台电脑每隔 10 分钟就会生成一个新的 EXCEL 文件，每个 EXCEL 文件记录了过去 10 分钟内所有的交易。并且这个 EXCEL 文件是在不断增加当中的，因为不断会有新的交易记录生成。

然后，在每个区块上，增加区块头，其中记录了父区块的哈希值。通过在每个区块存储父区块的哈希值，就可以把所有区块按照顺序组织起来，形成区块链。如下图所示，97 区块包含了一个区块头和一些交易记录，这些加起来，实际上都是一些文本，我们将这些文本内容打包，打包之后计算一个哈希值。这个哈希值就是整个 97 区块的哈希值，然后将这个哈希值记录在 98 区块的区块头里面。每个区块都如此操作。每个区块的区块头，都存储父区块的哈希值。这样就将所有区块按照顺序连接了起来。最终形成了一个链条，就叫区块链。



我们可能会问，第一个区块的前面没有区块了，那么它的区块头记录什么信息呢？第一个区块的区块头其实不记录前一个区块的信息，所以第一个区块是一个比较特殊的区块，我们称之为创世区块。之前我们曾经讲过，2009 年 1 月 3 日，在位于芬兰赫尔辛基的服务器上，至今匿名的神秘技术极客中本聪生成了第一个比特币区块，即所谓的比特币“创世区块”。

我们把原来一个很简单的账本，搞得这么复杂，这是为什么呢？这其实就是为了解决我们比特币要解决的第一个问题，就是要保证我们的交易记录不被篡改。

那么，区块链是如何防止交易记录被篡改的呢？

假设我们修改了区块 98 的一点内容，这个时候，当有其他人来检查的时候，他很容易就可以发现，区块 99 中已经记录的关于区块 98 的哈希值，和最新计算得到的区块 98 的哈希值，二者不一样了。他就可以知道，区块 98 已经被修改过。假设修改区块 98 的人的权限很大，他不仅把区块 98 的内容修改了，他还同时把区块 99 中的区块头的内容也修改了，那么实际上，我们也能够发现篡改信息的行为。因为区块 99 的头部被修改了以后，重新计算得到的区块 99 的哈希值，就和保存在区块 100 中的头部的哈希值，二者不同了。假设这个篡改的人很厉害，他把信息一致篡改下去，不仅改 98 区块，也改了区块 99 的头部，也改了区块 100 的头部，一直改下去，一直改到最后一个区块，也就是最新的一个区块，那么也没有什么问题。因为，他只有获得最新区块的写入权，才可以做到。而要想获得最新区块的写入权（也就是记账权），他就必须控制网络中至少 51%的算力。但通过硬件和电力控制算力的成本十分高昂。比如，以 2017 年 11 月 16 日的价格计算，在比特币网络进行 51%攻击，每天的成本包含大约 31.4 亿美元的硬件成本和 560 万美元的电力成本。

因此，我们可以说，区块链能够保证里面记录的信息和当时发生的时候一模一样，中间没有发生篡改。

所以，比特币和区块链的本质：就是一个人人可见的大账本，只记录交易。区块链的核心技术是通过密码学和数据结构，保证账本记录不被篡改。区块链的核心功能是创造信任。货币的本质就是信任。使用纸币和黄金，就是因为信任。法币依靠政府公信力创造信任，比特币则依靠区块链技术创造信任。

2、在比特币的世界中如何进行交易

现在，我们来看一下，在比特币的世界中，如何进行交易？

进行交易，需要账号和密码，分别对应于公钥和私钥。在比特币中，私钥是一串 256 位二进制数字。获取私钥不需要申请，甚至不需要电脑，可以抛硬币 256 次来生成。地址由私钥转化而成，但是，根据地址不能反推出私钥。地址即身份，代表了比特币世界的 ID。一个地址（私钥）产生以后，只有进入区块链账本，才会被大家知道。

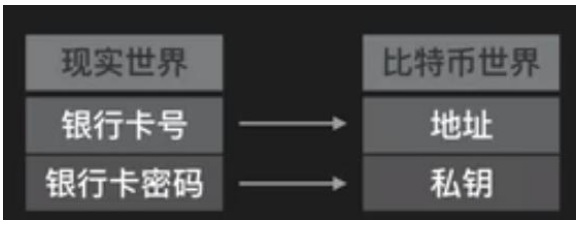
为了方便理解，可以做个比喻，比特币世界中的地址，就相当于现实世界中的银行卡号，比特币世界中的私钥就相当于现实世界中的银行卡密码。但是，它们之间还是有一些区别的，具体如下：

（1）银行卡密码可以修改，但是，私钥一旦生成，就无法修改；

（2）银行卡需要申请，而地址和私钥自己就可以生成；

（3）银行卡实名制，地址和秘钥是匿名的；

（4）个人申请银行卡有限制，但是地址和私钥可以无限生成。



张三已经有了地址、私钥，想要转账给李四 10 元，如何将这条交易记录添加到区块链中呢？

在把一条交易记录添加到区块链之前，首先就需要确认交易记录的真实性，这时就需要用到数字签名技术。如下图所示，张三调用签名函数 Sign()对本次转账进行签名，然后，其他人通过验证函数 Verify()来验证签名的真实与否。也就是说，张三通过签名函数 Sign()，使用自己的私钥对本次交易进行签名，任何人都可以通过验证函数 Verify()，来验证此次签名

是否由持有张三私钥的张三本人发出的（而不是其他人冒用张三的名义），是就返回 True，反之返回 False。Sign()和 Verify()由密码学保证不被破解。

签名函数的执行都是自动的，并不需要我们手工去处理这些事情。比如我们安装了比特币钱包 APP，它就会帮我们去做这样的事情，因为钱包 APP 是知道我们的私钥的，所以，我们只要告诉这个 APP，我想转账 10 元给李四，那么这个钱包 APP 会帮我们自动生成这次转账的信息以及签名，然后向全网发布，等待其他人使用 Verify()函数来验证。

这里需要重点强调的是，在比特币世界中，私钥就是一切。首先你的地址是由私钥产生的，然后你的地址上有多少钱，别人都是知道的，因为这些账本都是公开的。然后，只要他知道你的私钥，那么，他就可以发动一笔交易，把你的钱转到他自己的账户上面去。所以，一旦丢失了私钥，就丢失了一切。它不像银行卡一样，银行卡如果别人知识知道了你密码是没有用的，还要知道你的卡号。而且你还可以挂失银行卡。但是，在比特币的世界中，一旦你丢失了私钥，你就什么都没有了。所以，如何保管你的私钥，是一个很有讲究的问题，很多人都因为丢失了私钥，而造成了很大损失。

以私钥为代表的区块链金融科技，成为旧时代的掘墓人和新时代的奠基人。拥有私钥便拥有一切，未来家庭的保险柜里，储存的不再是黄金和美元，而是便签纸上记下的一串串私钥；财产的传承，也不止是股票和债权，还有见证亲密程度的私钥；新婚燕尔的男孩上缴的不再是工资卡，而是私钥；婚姻围城中无处容身的男人所藏的，不再是私房钱，仍是私钥。

3、在比特币的世界中由谁负责记账

【去中心化记账】

一条交易记录的真实性得到确认以后，接下来的问题是，由谁负责记账呢？也就是说，由谁负责把这条交易添加到区块链中呢？

首先，我们就会想到，由银行、政府或支付宝这些权威机构负责记账，也就是采用“中心化方式”来记账。然而，历史上所有由中心化机构记账的加密数字货币尝试，都失败了。因为中心化记账的缺点很多，主要如下：

（1）拒绝服务攻击。对于一些特定的地址，记账机构拒绝为之提供记录服务。

（2）厌倦后停止服务。如果记账机构没有从记账中获得收益，时间长了，就会停止服务。

（3）中心机构易被攻击。比如破坏服务器、网络，监守自盗，法律终止，政府干预。

正是因为中心化记账会存在很多问题，因此，比特币需要解决第二个问题：去中心化。

在比特币区块链中，为了实现去中心化，采用的方式是：人人都可以记账，每个人都可以保留完整账本。任何人都可以下载开源程序，参与 P2P 网络，监听全世界发送的交易，成为记账节点，参与记账。当 P2P 网络中的某个节点接收到一条交易记录时，它会传播给相邻的节点，然后相邻的节点再传播给其他相邻的节点，那么通过这样一个 P2P 的网络，这个数据会瞬间传遍全球。

采用去中心化记账以后，具体的分布式记账流程如下：

（1）某人发起一笔交易以后，他向全网广播；

（2）每个记账节点，持续监听、传播全网的交易。收到一笔新交易，验证准确性以后，将其放入交易池，并继续向其他节点传播；

（3）因为网络传播，同一时间，不同记账节点的交易池不一定相同；

（4）每隔 10 分钟，从所有记账节点当中，按照某种方式抽取 1 名，将其交易池作为下一个区块，并向全网广播；

（5）其他节点根据最新的区块中的交易，删除自己交易池中已经记录的交易，继续记账，等待下一次被选中。

【去中心化记账的特点】

比特币的去中心化记账有什么特点呢？

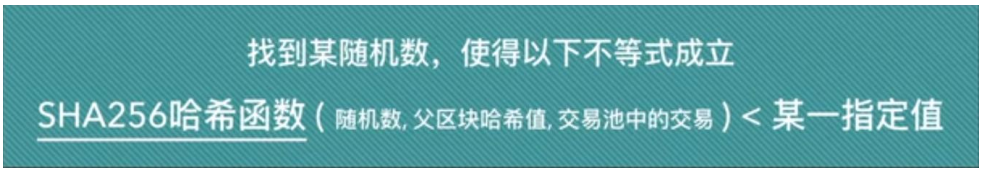
（1）每隔 10 分钟产生一个区块，但是，并不是所有在这 10 分钟内的交易都会被记录。这个比较好理解，我这笔交易是在这个 10 分钟内发生的，但是，不一定会在这 10 分钟之内被记录，我有可能是在下一个 10 分钟之内被记录，也有可能是在下下个 10 分钟之内被记录，这主要是因为一笔交易在 P2P 网络中的传播需要时间，可能在这个 10 分钟之内被选中的节点，它还没有接收到这笔交易的信息，所以，这笔交易就不能在这个 10 分钟之内被记录到区块链里面。

（2）获得记账权的记账节点，会获得 50 个比特币的奖励。每隔 21 万个区块（大约 4 年）以后，奖励减半。总量约 2100 万枚，预计到 2040 年可以开采完。2009 年比特币诞生的时候，每笔赏金是 50 个比特币。诞生 10 分钟后，第一批 50 个比特币生成了，而此时的货币总量就是 50。随后比特币就以约每 10 分钟 50 个的速度增长。当总量达到 1050 万时（2100 万的 50%），赏金减半为 25 个。当总量达到 1575 万（新产出 525 万，即 1050 的 50%）时，赏金再减半为 12.5 个。而随着比特币减半，矿工们压力更大，算力升级要求更高。

（3）记录一个区块的奖励，也是比特币的唯一发行方式。

【如何分配记账权】

在上面的分布式记账的步骤中，还有一个很重要的问题需要讨论，那就是，如何分配记账权。在比特币区块链中，采用的是 POW 机制，也就是“工作量证明机制”。记账节点通过计算如下数学题，来争夺记账权：



上面这个数学公式的计算，除了从零开始遍历随机数碰运气以外，没有其他办法。解题的过程，又叫挖矿，记账节点被称为矿工。谁先解对，谁就获得记账权。某记账节点率先找到解，就向全网公布，其他节点验证无误之后，在新区块之后，重新开始下一轮计算，这种方式被称为 POW。

4、比特币世界中的“挖矿”

【挖矿】

比特币也效仿黄金领域：获得比特币的方式叫“挖矿”，挖比特币的计算机，被叫做“矿机”。所谓“矿工”，即通过完成计算题来获取比特币的人。所谓“挖矿”，就是每 10 分钟就会有一道数学题被扔到网络中，大家比赛，看看谁算得快。算得最快的计算机，就会“挖”到一定数量的比特币，矿工们通过为比特币网络提供“算力”来换取获得比特币奖励的机会，算力越多的计算机，得到越多的比特币。

打个简单的比方，我手上现在有一张面值 100 元的人民币，谁猜出来编号我就给谁。比特币就等于这张钱，猜编号就等同于挖矿，谁猜对的速度最快，这 100 元就是谁的。

获得记账权的概率其实是很好算的。假设我这个节点每秒钟计算哈希函数的次数是 1 亿次，然后我知道，全网所有节点他们每秒钟计算哈希函数的次数是 100 亿次，那么我这个节点争取到记账权的概率就是 1%。因此，为了以更高的概率获得记账权，我唯一的办法就是找来更多的机器，这些机器可以让我每秒钟去运算的次数更多。这也是大家了解到的，矿工不断地去购买更好的矿机去投入到挖矿的过程。

【电脑挖矿】

刚开始的时候去挖矿，你使用传统电脑的 CPU 就可以挖矿，因为全网的算力其实不是很高，之后呢，随着全网算力越来越高，你希望得到更多的记账权，你也得提高你计算的速度，所以大家改成使用 GPU 来挖矿。再之后就升级为专业的矿机，这个实际上就是一场军备竞赛。很多矿机在购买来几个月以后，它的计算能力就很快被淘汰了，因为速度太慢。

在比特币发展过程中，就出现了“挖矿木马”。一些来路不明的文件，你在电脑上随手一点，你的电脑就有可能成为黑客团伙挖矿的苦力。当你发现电脑突然严重卡顿，可能它正在为暗处的黑客掘金。

【矿机挖矿】

随着专业矿机的出现，个人电脑基本已经在这场挖矿游戏中被淘汰出局。举个例子，挖地铁，专业矿机好比是盾构机，挖三个月贯通，获得 1 比特币的奖励。而你家里的电脑，相当于一把勺子，挖条地铁出来，得多少年？实际上矿机的算力不会比家用电脑强这么多，有点太夸张，但是数万倍的算力差距是有的，这还没有用几百万一台的超级矿机来做对比。

如下图所示，就是一台专业的矿机。成本只有 9000 多元的矿机，最高一台卖到了 26 万元，足见当时市场需求的强烈程度。市面上功耗较大的矿机神马 m3，算力是 11.5t （1T 是 1 万亿次浮点指令每秒），功耗是 2150w，二十四小时运行情况下单台耗电量：2.15 千瓦*24=51.6 度。

随着大量矿机的加入，比特币全网算力迅速增长。这种指数级别的增长，正面临“失控”着状态。目前比特币矿业消耗电力已经超过整个大英帝国的用电量。研究机构曾做出过这样的统计：如果按照 2018 年 11 月份“比特币挖矿耗电量”增长速度来计算，到 2019 年 7 月，

比特币挖矿耗电量将超过如今美国全国的一年用电量。

一些环保主义者认为，比特币是一种投机资产，是资本主义晚期的产物，因为它消耗了大量的电力，但对社会并没有真正价值，甚至有人将其称为自由主义的“泔水”。

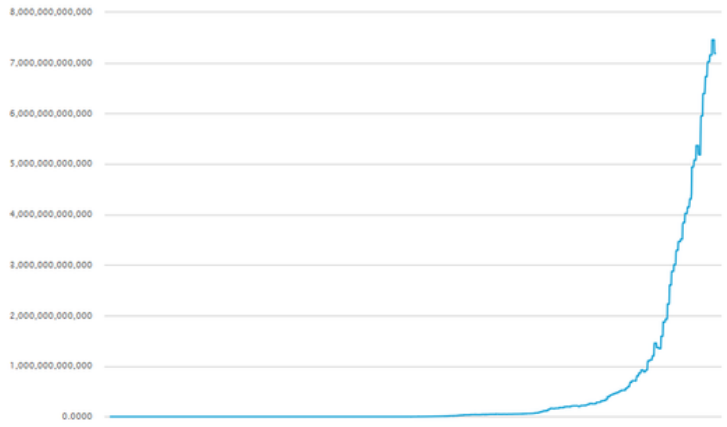
【矿机生产公司上市】

2019 年 11 月 21 日，区块链第一股、全球第二大加密货币矿机生产商嘉楠耘智，在美国纳斯达克上市。

截至 2017 年 4 月末，嘉楠耘智累计售出阿瓦隆系列矿机约为 16 万台，占据了全球比特币算力市场的 22%，如果说比特大陆吴忌寒（见下图）是矿机市场最具影响力的人，那嘉楠耘智的掌舵人张楠赓毫无疑问就是行业第二。

【比特币全网算力】

这么多专业矿机的加入，使得比特币全网算力迅速提升（如下图所示），那么，会不会影响每个区块链生成的时间呢？答案是，不会的，每个区块链生成的平均时间依然是 10 分钟左右。因为，随着全网的算力不断变化，为了应对算力的变化，每隔 2016 个区块（两周），会加大或减少难度，使得每个区块产生的平均时间是 10 分钟。这里需要额外说明的是，每个区块产生时间并不是正好 10 分钟。因为，有时候，某个节点运气特别好，它很快就找到了随机数答案。而有时候，运气又特别差，隔了很长时间（20 分钟甚至 30 分钟）才找到随机数答案。其实这都是一个概率问题。



（上图 2010 年以来比特币全网算力增长情况）

比特币的出币速度是固定的，挖矿的人多了，挖矿难度就升高。随着比特币全网算力的不断提升，挖矿的难度也在不断增加。就目前比特币的挖矿难度来看：

比特币（btc）每 t 收益：1TH/S*24H=0.00007087btc

按综合 12t 的机器算力来算每天产量为：

0.00007087*12t=0.00085044btc

那么单台挖到一个 btc 的时间需要：

1/0.00085044=1175 天

十台矿机挖到一个 btc 的时间需要：

1/0.0085044=117 天

一百台矿机挖到一个 btc 的时间需要：

1/0.085044=11.7 天

也就是说，按照目前的难度来算，大概单台矿机需要三年的时间可以产出一枚比特币，十台矿机需要 3.9 个月可挖一个比特币，一百台矿机只需要 11.7 天可挖出一个比特币，投入单台机器成本价 8500 左右，十台在 85000 左右，一百台投入 850000，不到一百万，一个月收入超过两枚比特币，按目前的币价来算大概价格十二万，如此看来，目前比特币挖矿的收益虽然不及之前，但相较于其他投资项目还是很可观的。

【矿场】

大量的矿机可以集中存在一个矿场里面。下图是北美最大的矿场。

集中先进矿机和低廉电费的中国，目前是全球加密货币矿场的首选地之一，有多达 7 成的比特币算力分布在四川、云南、内蒙古、新疆等地。下图是坐落于四川省某电站旁边的矿场。

【为什么都来中国建立矿场】

在中国，加密货币的挖矿产业已经形成了一条完整的产业链上下游，目前我国已经是生产全球 9 成的矿机，占有 7 成比特币算力，运营着超过一半的矿场，拥有庞大从业者人群的重要产业基地。

中国有比特币网络中超过 75%的矿池，这导致中国成为比特币网络中的一个无比重要的国家，你可以想象到，如果中国全面禁止挖矿的话，会产生多大的影响。可以说，中国对挖矿的政策会直接关系到比特币的存亡。这就是为什么中国的每一条关于比特币的消息、新闻或政策都会让各方人物高度关注。

世界上多数加密货币行业的矿机制造公司都在中国发展，全球比特币矿机排名第一的比特大陆的总部就在北京，计算机芯片的硬件制造这方面在世界上几乎没有竞争对手。它还负责在全球运输数十亿的采矿设备，这数量已经占了行业内可运行矿机的四分之三了。

为什么比特币矿场大都选择在中国建立？

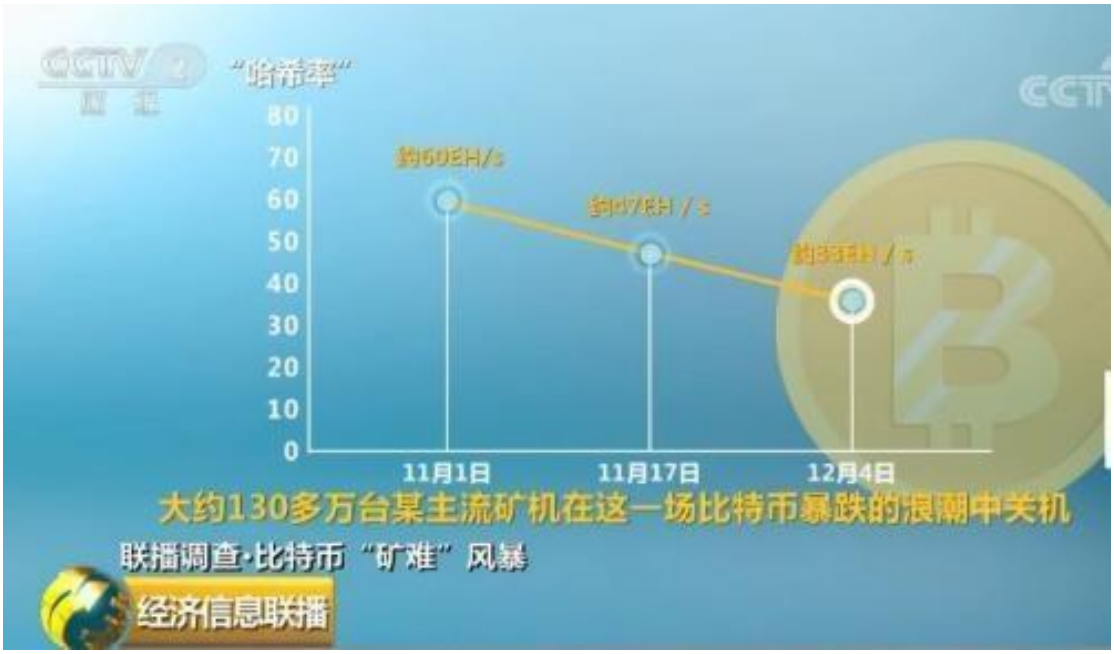
今天的挖矿形式已经不再像之前那样，靠一张显卡或者几台矿机就足以完成任务了，现

在的挖矿所需要的算力已经到了一个非常高的地步，以至于现在都只能以矿池的形式存在。矿池的算力是包含了各个矿场、诸多矿工的算力集中起来的，不同的矿场、不同的矿工聚集在一个矿池，为这整一个矿池提供算力。这样，挖矿的效率高了许多，挖到区块之后按照贡献出来的算力比例分成比特币奖励。这很好的说明了为什么大家都要聚集在中国建立矿场，因为中国有良好的环境和低廉的电费成本。在中国，有许多地方都会出现电能过剩的情况，这会导致电费十分廉价，许多过剩的电能都会以十分便宜的价格出售给矿场使用。所以即使是在被称为挖矿天堂的伊朗，挖矿成本仍然要高于中国。同时，中国政府对挖矿的监管比较放松，这对于广大矿场主来说也是一个很大的优势。尽管中国政府早就对加密货币这块做出了许多禁令，如禁止国内有比特币相关的交易所、禁止 ICO 等，但尚未明确禁止挖矿。因此，经过多因素综合考虑，中国确实是非常适合进行相关的挖矿操作，以至于全球的矿机生产商、矿场主纷纷来到中国开展业务。

【矿难】

在现实世界中，挖矿时遇到矿难是在所难免的。同样，在比特币的世界中，在挖矿的过程中，也会遇到矿难。所谓矿难，就是挖矿的收益小于挖矿的各种投入。

下图是央视的新闻报道，在比特币市场行情不好的时候，也就是发生矿难的时候，大约 130 万台某主流矿机在一场比特币暴跌的浪潮中关机。



深圳的华强北是全世界最大的矿机销售集散地，全球约 9 成的矿机都是从那里发货。半年多前的华强北，无论是卖电脑配件还是手机内存的商家都纷纷做起了矿机销售生意。

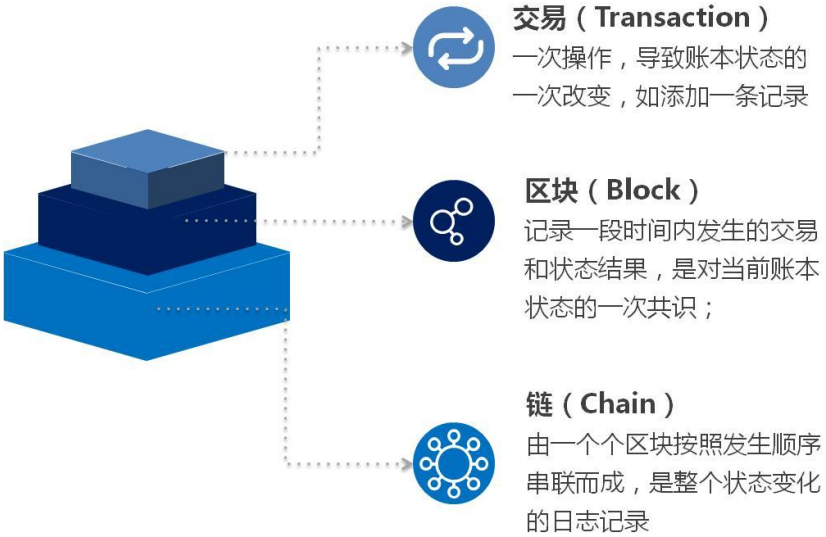
随着比特币价格暴跌，目前某主流型号的矿机，价格已经跌去 95%，但依然卖不出去。深圳矿机销售商：有些客户之前在我这买的矿机，现在要卖。几个月前花 3 万多买的，现在只能卖到 800 到 1100,1200 左右。

【比特币全貌】

讲到这里，总结一下，比特币的全貌就是，采用区块链（数据结构+哈希函数），保证账本不能被篡改；采用数字签名技术，保证只有自己才能够动自己的账户；采用 P2P 网络和 POW 共识，保证去中心化的运作方式 。

【区块链三要素】

区块链的三要素是：交易、区块和链，具体如下图所示。



这里，给区块链一个完整的定义：区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

【区块链分类】

区块链包括公有链、联盟链和私有链。

（1）公有链：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。公有链通常被认为是“完全去中心化”的。

（2）联盟链：对特定的团体开放的区块链，介于公有链和私有链之间。某种程度上也划归为私有链。这个例子很多，比如 Libra 就是和 28 家国际级支付机构共同打造的联盟链。最近，光大银行联合中国银行、中信银行、民生银行、平安银行等基于区块链技术共同打造的“福费廷交易平台（BCFT）”也是一个联盟链，所谓福费廷交易平台简单理解就是票据及其衍生品的交易平台。

（3）私有链：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。比如，某社区需要选举，于是开发一个基于区块链技术的投票系统，社区内部所有人都可以在链上投票，但这个链只对社区内部和开发者透明，而且使用者可以匿名，控制权在社区主管机构，使用者只是参与者。可以看出，私有链是一个不完全去中心化的区块链，许多人认为区块链如果过于中心化，那就跟其他中心化数据库没有太大区别。

【区块链重要意义】

区块链的重要意义表现在：

（1）区块链，是互联网的二次革命。

（2）区块链，是互联网 2.0。

（3）区块链，让我们从信息互联网跨越到价值互联网。

从 1994 年互联网开始商业化，经过近 25 年的发展，互联网已经彻底改变了我们周围的一切——经济、产业、生活。互联网从 1995 年左右的“信息高速公路”的说法，变成了无处不在的力量。现在，如果区块链是互联网 2.0，互联网曾经带来的改变以区块链的方式再来一次，随着区块链技术的进步和相关基础设施的完善，各种意想不到的应用会涌现出来。

三、区块链相关概念

1、智能合约

智能合约又称智能合同，是由事件驱动的、具有状态的、获得多方承认的、运行在区块链之上的、且能够根据预设条件自动处理资产的程序，智能合约最大的优势是利用程序算法

替代人仲裁和执行合同。

简单地说，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。智能合约就是传统合约的数字化版本。

尼克·萨博最早于 1994 年提出了智能合约。尼克·萨博说：“智能合约的设计目标是，执行一般的合同条件，最大限度地减少恶意和意外的状况，最大限度地减少使用信任中介。”他认为，我们需要一个这样的计算机协议：它能够完全保证，如果付款了，商品会被发送，或者商品寄出去了，就会收到钱。

在现实生活中，我们有很多办法来实现这一点。而计算机科学家的目标是，用事先确定的代码自动执行合约条款，无须人工干预和第三方中介。

智能合约中的“智能”可以理解为，按条件自动执行，无须人的干预，是自动的或自治的。智能合约贴切的形象类比，是我们在说起计算机术语“有限状态机”或“状态机”时常用的自动可乐售卖机：我们向可乐售卖机投入硬币，按一下出可乐的按钮。售卖机将一听可乐从出货口放出来。售货机恢复到最初的状态。

萨博就认为，所有的交易合同都没有必要通过第三方完成，只要合同的条款可以用编程语言来表达，让计算机自动处理就行了。这样就避免了合同执行中的尔虞我诈，还节约了大量的交易成本。

这个设想当然是很天才的。但是，你发现没有，它里面有两个漏洞。

第一个，交易是要涉及到资产的转移的，假如说一个交易完成以后，资金的转移还要到银行去进行，那就丧失了智能的意义了。所以，为了全程实现计算机的控制，交易的资产必须是以数字资产的方式存储和呈现。

第二个，计算机程序存在着被篡改的风险。所以，怎么确定合约条款的可信度也是个大问题。

就因为这两个原因，在萨博提出智能合约这个概念以后，很长时间内就停留在自动售货机、自动售票机这种比较初级的模式上，没有找到真正的突破口。

尼克萨博关于智能合约的工作理论迟迟没有实现，一个重要原因是缺乏能够支持可编程合约的数字系统和技术。

区块链技术的出现解决了该问题，不仅可以支持可编程合约，而且具有去中心化、不可篡改、过程透明可追踪等优点，天然适合于智能合约。

将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障存储、读取、执行整个过程透明可追踪、不可篡改。同时，由区块链自带的共识算法构建出一套状态机系统，使得智能合约能够高效地运行。

这就是智能合约与区块链的关系，简单总结来说智能合约早期提出缺乏支持可编程的数字系统技术，区块链的出现解决了该问题，不仅可以支持可编程合约而且可以去中心化，不可篡改，过程透明，可追踪的优点天然适合智能合约。

智能合约的工作原理包括三个部分：

（1） 智能合约的构建：由区块链内的多个用户共同参与制定一份智能合约；

（2） 智能合约的存储：智能合约通过 P2P 网络扩散到每个节点，并存入区块链；

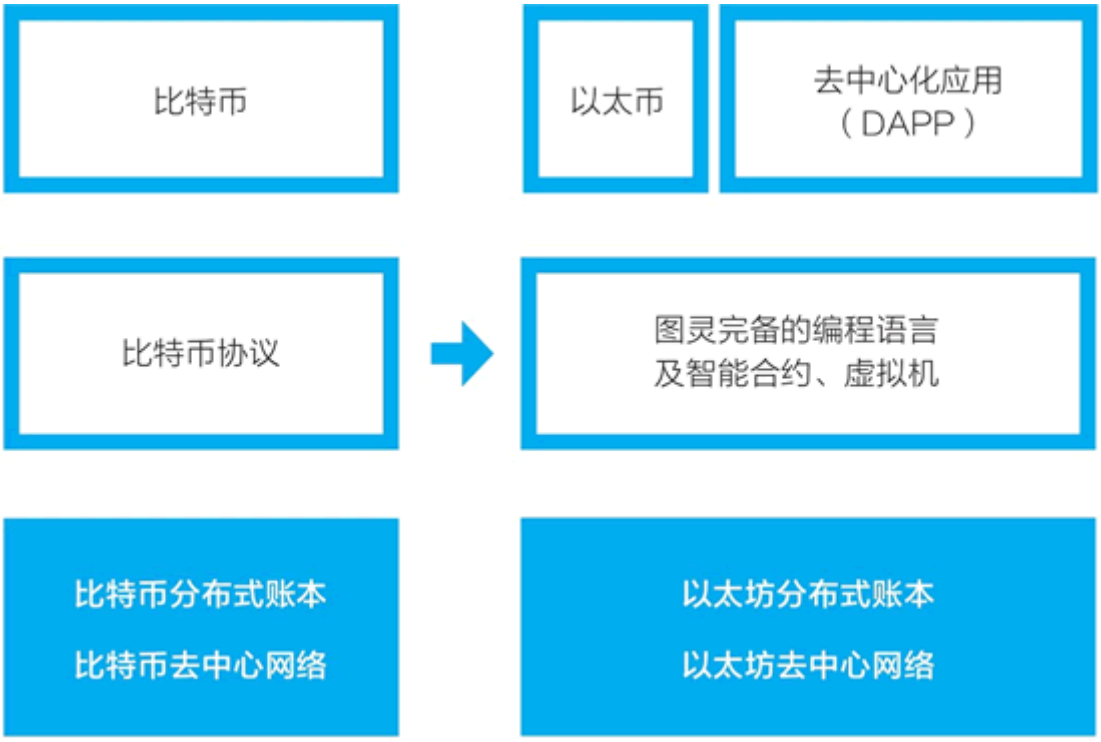
（3） 智能合约的执行：智能合约定期执行自动机状态检查，将满足条件的事务进行验证，达成共识后自动执行并通知用户。

2、以太坊

以太坊在比特币底层技术“区块链”的基础上，加入了“智能合约”的概念，加速了区

块链技术在金融行业的广泛探索。纽约梅隆银行、花旗银行、汇丰银行、三菱 UFJ 等多个国家的主流银行加入其中，传统金融机构开启了以区块链技术为支撑的新一代金融基础设施的搭建。2014 年 7 月，以太坊成功募集 3 万余个比特币，以当时的汇率约合 1840 万美元。刚刚过去的 2017 年，以太坊的市值已突破 790 亿美元。

如果以太坊能顺利地完成第二次革命，在保持去中心化和安全的前提下，完成可扩展性方案，那么，以太坊势必成为未来全球经济的底层结算层，分布式架构和经济激励体系如同珍贵无比却免费的阳光、水和空气，促使无数的银行、证券交易所、保险公司等诞生其上，以太坊不是要取代华尔街，而是要催生出无数的华尔街。



3、ICO

“区块链/比特币”大爆发之后，有几个必然的结论：

（1） 区块链很厉害，会颠覆很多行业；

（2） 基于区块链的数字货币，有天然的金融属性，可创造、可交易，可现货、可期货……

（3） 一个比特币是无法满足大家的需求的，很多人希望自己创造出独一无二的区块链和数字货币项目。

于是很多人钻研于此，在很多庄家、大咖的护航之下，市场终于爆发，直接导致了 ICO 这个概念在 2017 年上半年突然变得炙手可热。

ICO 是（Initial Coin Offering）的缩写，它跟 IPO（Initial Public Offering）不但看起来类似，意思也差不多。IPO 是首次公众发行，ICO 则是首次币发行。

ICO 是一种为区块链项目筹集资金的方法，它不是把公司股权拿出来发行，而是把区块链项目对应的数字货币拿来发行，收取的也是通用的数字货币，通常为比特币或者以太币。

随着区块链项目正式上线，代币在虚拟货币交易所上市交易，投资者可以通过出售代币

实现投资退出。代币价格的涨跌与传统的证券流通市场类似，会反映出公司的公众认知度、增长潜力，甚至被用于炒作。

ICO 有两点创新：第一，让创业全球化：全球化募资、全球化投资、全球化项目、全球化参与；第二，它在弥补两种融资方式的鸿沟，从个人机构贷款到股市，中间有很多公司无法融资。所以 ICO 是一个很重要的工具，会在下个十年完全改变创业公司的运转方式。它会颠覆风险投资、股票市场，早期投资。

从前如果我想做个区块链的创业项目，一般的流程是先着手组队推进项目，同时准备商业计划书，四处找投资人，那股权换来投资，顺利的话，ABCD 轮这样一步步走下去。

但 ICO 就完全不同了，直接颠覆了以往的融资方式。**不需要你注册公司，不需要你的产品原型、收入等等，可能只是随便几页项目白皮书，甚至只有一个项目愿景，发行一个“xx币”，**出售一小部分，就能够换来价值几千万甚至上亿美元比特币或者以太币，无数人哭着喊着要投钱进来，这是人类历史上从未出现的景象。人称“比特币首富”的李笑来创立名为 EOS 的区块链项目，仅用 5 天时间就在 ICO 平台上融到了 1.85 亿美元，巅峰时刻更是在对应的二级市场市值冲到 50 亿美元，让所有投资者都激动不已。

参与到 ICO 中的大概有三种人：

（1）第一种，是真正的投资人

真懂区块链、真懂投资。他们真相信这个“xx 币”背后的区块链项目是能解决真实问题的，这个团队最终是能做得非常好，赚到大钱的。**对他们来说，他们投的是项目，**只是以前投美元、投人民币，现在投比特币，投以太币。

（2）第二种，是投机者

这些投机者把“xx 币”当作股票，把 ICO 当成 IPO，投资当成打新股。反正只要有人用更高的价格接盘，就能赚到钱。这个区块链项目未来是死是活跟我无关，赚一把就走。**玩的是击鼓传花的游戏并确信最后的受害者不是自己。**

（3）第三种，是跟风者

他们什么都不懂。只是被这个热潮裹挟或者受了某些人的蛊惑**跟风进来的，**在超高利润的诱惑下去体验一种自己都觉得不真实的快乐。

投资人、投机者，跟风者的扎堆，吸引了行骗者大举进军 ICO，像亚欧币这种项目短时间募集 40 亿，而项目完全子虚乌有。

由于交易中 ICO 使用数字货币，融数字货币，所用到的双边都是数字资产，所以目前一直处于监管的真空之中。**因为 ICO 的交易者必须使用比特币或者以太币，这又进一步推高了比特币的价格。**

比特币又多了一个使用场景，这进一步加强了数字货币的愿景，形成正向激励，导致数字货币鸡犬升天，各种暴富神话充斥坊间，ICO 投资迅速过热，乱象丛生。

这也直接导致监管出手，然后 ICO 在中国就偃旗息鼓了，可区块链和数字货币的高潮还在持续，鱼龙混杂，其中有的公司可能未来有千亿市值，有的可能抱着捞一把就走的骗子，**这个市场还需时间。**

但目前的区块链项目有多少靠谱的呢？99%的可能都会死去，ICO 这个玩法有点挑战人性，奋斗后有成果是一种激励，而没开始奋斗就拿到巨大的财富，是否有动力去实现白皮书宣称的事情确实不好说。

更有甚者，那区块链和数字货币作为一种骗术，数额巨大，隐蔽性强，所以大多数人难逃韭菜的命运。

ICO 所发行的数字货币，与比特币们有着根本不同，比特币如同黄金，总量以及流动，不受任何单独一方控制，或者说是被多方控制，是去中心化的。但是 ICO 是中心化的，发行

之初，就设计了自身利益最大化的方案。

至于政府为何禁止 ICO？有两个原因。

第一，怕泡沫破裂破坏社会稳定。但要知道很多人加入 ICO 就是为了投机、卖出找人接盘的。投资者要对自己负责，不需要父爱主义的政府。

第二，ICO 技术本身的确颠覆了政府管控下的 IPO 融资方式，在和传统体系下的融资方式竞争，正如比特币和法币体系竞争一样。

下图给出了目前融资最高的九大 ICO 项目。在短短的两年时间，全球有三起 ICO 筹集资金超过 2 亿美元，另有 6 起 ICO 超过 1 亿美元。值得关注的是，其中 8 起融资都发生在 2017 年：随着数十亿资金涌入新项目，投资者和投机者正在焦急地等待，看哪一个代币将成为下一个席卷市场的以太坊。

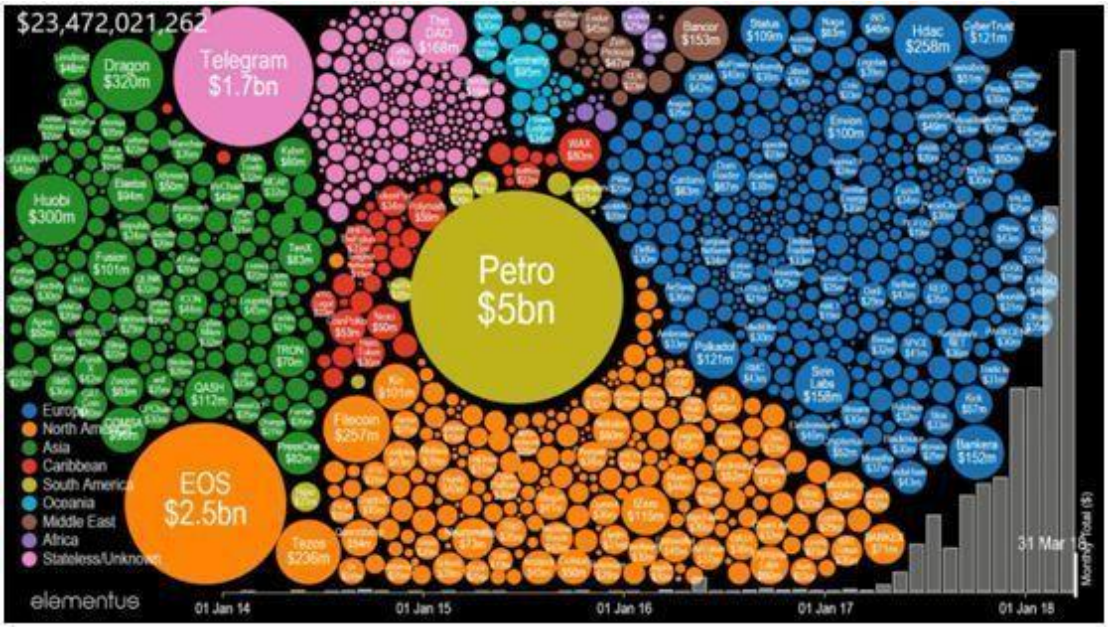
融资最高的九大ICO项目

名称	地区	募集资金(美元)	ICO时间
Filecoin	北美	2.57亿美元	2017
Tezos	欧洲	2.36亿美元	2017
EOS	北美	2亿美元	2017
Paragon	北美	1.83亿美元	2017
The DAO	无国界	1.68亿美元	2016
Bancor	中东	1.53亿美元	2017
Polkadot	欧洲	1.21亿美元	2017
QASH	亚洲	1.12亿美元	2017
Status	欧洲	1.09亿美元	2017

制表：资本实验室

资本实验室 www.coinsay.com

下面是 Elementus.io 制作的视频，描绘了自 2014 年初开始，截止 2017 年 11 月，全球区块链 ICO 融资的“细胞分裂”过程。这个无声而又让人叹为观止的视频，就像一部纪录片，记录了 ICO 从籍籍无名，到一飞冲天的狂热，也从侧面响应了 ICO 背后加密货币市场的一路高歌。



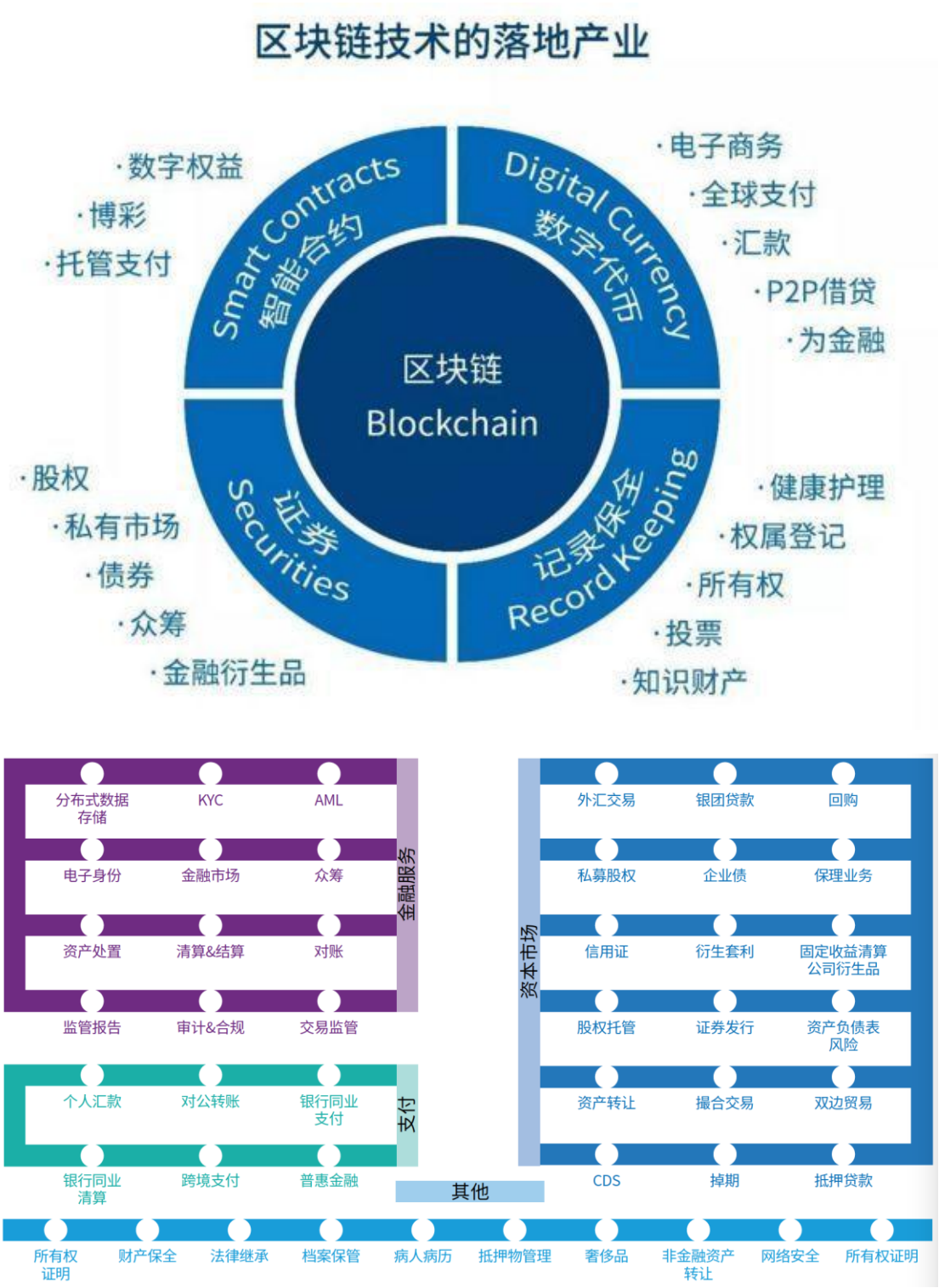
2017 年 9 月 4 日，央行等七部门发布《关于防范代币发行融资风险的公告》，叫停代币发行（ICO），要求已完成代币发行融资的组织和个人作出清退等安排。

如此大规模的清退，纠纷频发是必然现象。七宝网与政务链的“口水战”便是其中一个典型案例。2017 年 9 月 12 日晚，七宝网负责人张璐萍在直播间进行 ICO 维权，愤怒控诉前合作方——ICO 发行方政务链不配合工作，导致七宝网无法及时完成清退代币工作，并当场下跪。纠纷的焦点在于谁来承担 MIC（小米链）暴跌带来的损失，双方一直僵持不下。这就是现在中国 ICO 现状的一个缩影。

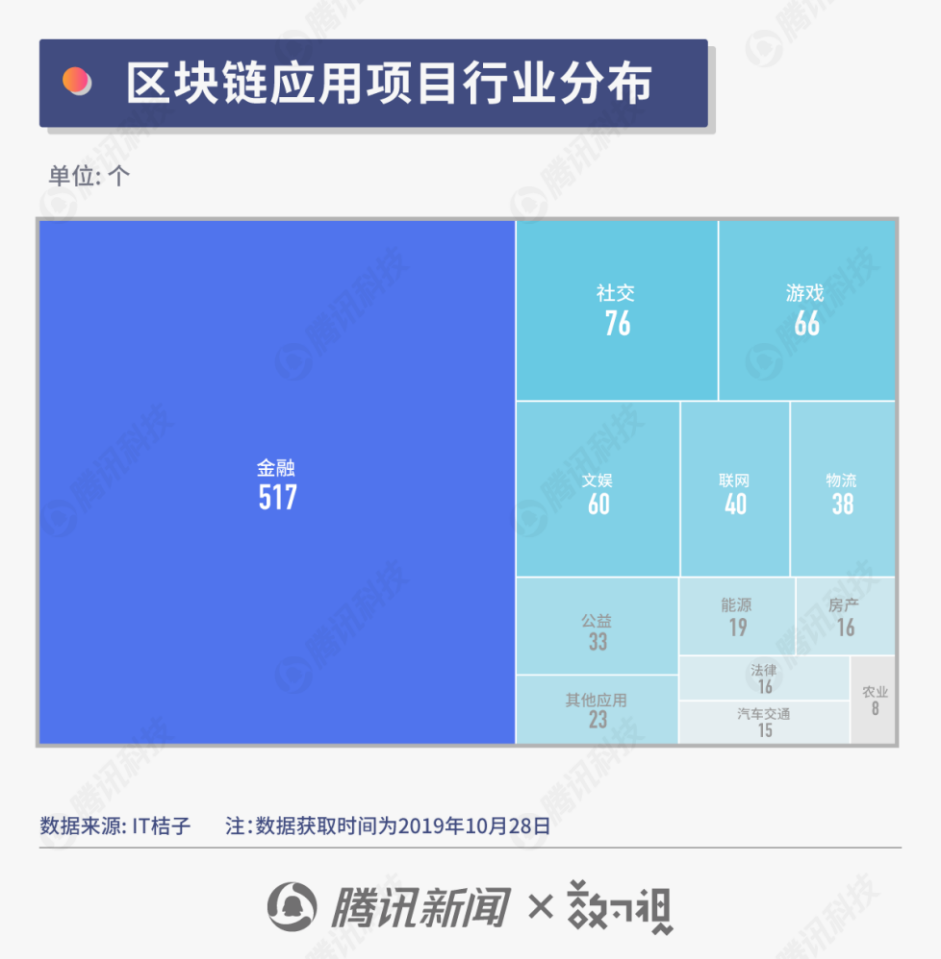
四、区块链应用场景

1、区块链应用概述

如下图所示，区块链在各行各业都得到了广泛的应用。

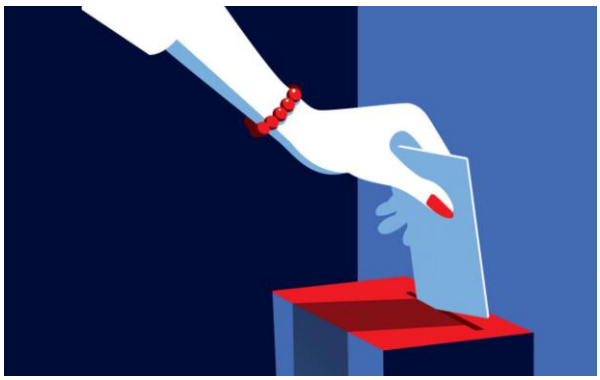


下图是区块链应用项目行业分布的情况，从中可以看出，金融业是区块链应用的主战场。



下图是区块链历年新增应用项目的情况。如果把 2008 年 10 月 31 日中本聪发布比特币白皮书作为区块链技术的生辰，2017 年则是区块链汹涌的青春期，一年之间新增应用项目达 321 个，至 2019 年 10 月，区块链应用项目达 984 个。

2、区块链应用场景：投票



举个例子，比如说**美国大选投票**，在美国大选中甚至出现一个事情，希拉里怀疑某一个投票站数字数错了，要求重选，为什么呢？因为是人工操作的，很多人在那里接收投票，然后再数票唱票。那么多州，那么多选票，那么多人参与选举，是有可能搞错的。所以大选是

中心化记账。

如果有一天所有人投票的时候，没有投票站，也没有人为此服务，而是所有人投票的时候，是向全美人民宣讲我投了他，所有的投票是被算法自动记录的，就不会犯任何的错误，这可能就会节省上万人的参与，大量的钱会省下来。

3、区块链应用场景：版权保护

（1）传统鉴证证明的痛点

- 流程复杂：以版权保护为例，现有鉴证证明方式，登记时间长，且费用高。
- 公信力不足：以法务存证为例，个人或中心化的机构存在篡改数据的可能，公信力难以得到保证。

（2）区块链 + 鉴证证明

- 流程简化：区块链应用到鉴证证明后，无论是登记还是查询都非常方便，无需再奔走于各个部门之间。
- 安全可靠：区块链的去中心化存储，保证没有一家机构可以任意篡改数据。

2016 年 8 月，由 Onchain、微软（中国）、法大大等多个机构在北京成立了电子存证区块链联盟“法链”。2017 年 12 月，微众银行、仲裁委（广州仲裁委）、杭州亦笔科技有限公司共同推出的仲裁联盟链，用于司法场景下的存证；2018 年 3 月，广州首个“仲裁链”判决书出炉。

4、区块链应用场景：物流链

（1）传统是防伪溯源手段

防伪信息掌握在某个中心机构中，有权限的人可以任意修改。以一直受假冒伪劣产品困扰的茅台酒的防伪技术为例，2000 年起，其酒盖里有一个唯一的 RFID 标签，可通过手机等设备以 NFC 方式读出，然后通过茅台的 APP 进行校验，以此防止伪造产品。 咋一看，这种防伪效果非常可靠。但 2016 年还是引爆了茅台酒防伪造假，虽然通过 NFC 方式验证 OK，但经茅台专业人士鉴定为假酒。后来，在“国酒茅台防伪溯源系统”数据库审计中发现 80 万条假的防伪标签记录，系防伪技术公司人员参与伪造；随后，茅台改用安全芯片防伪标签。

（2）区块链+物流链

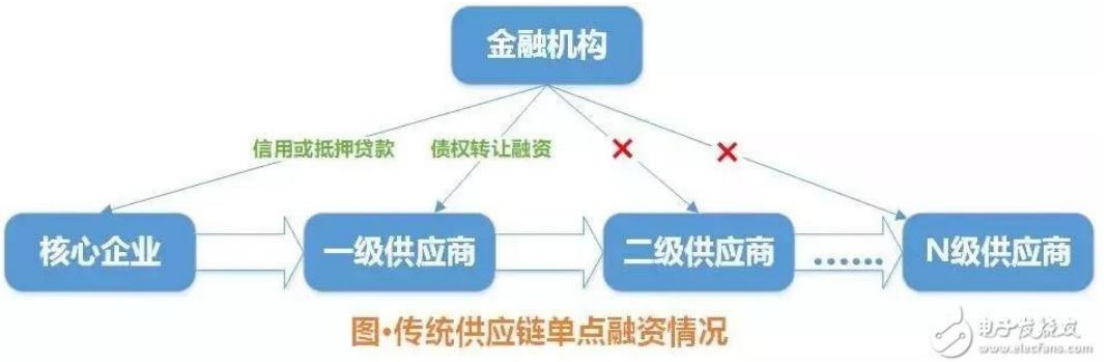
区块链没有中心化节点，各节点是平等的，掌握单个节点无法实现修改数据；

区块链天生的开放、透明，使得任何人都可以公开查询，伪造数据被发现的概率大增。

区块链的数据不可篡改性，也保证了已销售出去的产品信息已永久记录，无法通过简单复制防伪信息蒙混过关，实现二次销售。

物流链的所有节点上区块链后，商品从生产商到消费者手里都有迹可循，形成完整链条；商品缺失的环节越多，将暴露出其是伪劣产品概率更大。

5、区块链应用场景：供应链金融



图·传统供应链单点融资情况

在一般供应链贸易中，从原材料的采购、加工、组装到销售的各企业间都涉及到资金的支出和收入，而企业的资金支出和收入是有时间差的，这就形成了资金缺口，多数需要进行融资生产。

我们再来看看图中各个角色的融资情况：核心企业或大企业：规模大、信用好，议价能力强，通过先拿货后付款，延长账期将资金压力传导给后续供应商；此外，其融资能力也是最强的。一级供应商：通过核心企业的债权转让，可以获得银行的融资。其他供应商（多数是中小微企业）：规模小、发展不稳定、信用低，风险高，难以获得银行的贷款；也无法想核心企业一样有很长的账期；一般越小的企业其账期越短，微小企业还需要现金拿货。这样一出一入对比就像是：中小微企业无息借钱给大企业做生意。

面对上述供应链里的中小微企业融资难问题，主要原因是银行和中小企业之间缺乏一个有效的信任机制。

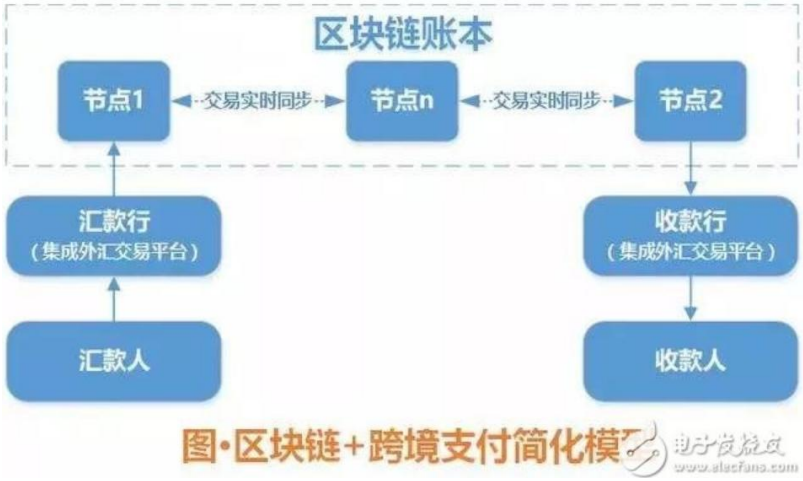
假如供应链所有节点上链后，通过区块链的私钥签名技术，保证了核心企业等的数据可靠性；而合同、票据等上链，是对资产的数字化，便于流通，实现了价值传递。

6、区块链应用场景：跨境支付

跨境支付涉及多种币种，存在汇率问题，传统跨境支付非常依赖于第三方机构，大致的简化模型如下图所示，存在着两个问题；流程繁琐，结算周期长：传统跨境支付基本都是非实时的，银行日终进行交易的批量处理，通常一笔交易需要 24 小时以上才能完成；某些银行的跨境支付看起来是实时的，但实际上，是收款银行基于汇款银行的信用做了一定额度的垫付，在日终再进行资金清算和对账，业务处理速度慢。手续费高：传统跨境支付模式存在大量人工对账操作，加之依赖第三方机构，导致手续费居高不下，麦肯锡《2016 全球支付》报告数据显示，通过代理行模式完成一笔跨境支付的平均成本在 25 美元到 35 美元之间。

图·传统跨境支付简化模型

如下图所示，区块链的引入，解决了跨境支付信息不对称的问题，并建立起一定程度的信任机制；带来了两个好处。效率提高，费用降低：接入区块链技术后，通过公私钥技术，保证数据的可靠性，再通过加密技术和去中心，达到数据不可篡改的目的，最后，通过 P2P 技术，实现点对点的结算；去除了传统中心转发，提高了效率，降低了成本（也展望了普及跨境小额支付的可能性）。可追溯，符合监管需求：传统的点对点结算不能不规模应用，除了信任问题，还有就是存在监管漏洞（点对点私下交易，存在洗黑钱的风险），而区块链的交易透明，信息公开，交易记录永久保存实现了可追溯，符合监管的需求。



图·区块链+跨境支付简化模

7、区块链应用场景：教育行业

在教育行业，学生身份认证、学历认证、个人档案、学术经历和教育资源等等都能够与区块链紧密契合。

比如说，可以将学生的个人档案、成绩、学历等重要信息放在区块链上，防止信息丢失和恶意篡改，这样一来，招聘企业就能够真实可靠地得到学生的个人档案，有效避免了学历造假等问题。

8、区块链应用场景：数字政务

区块链可以让数据跑起来，大大精简办事流程。

区块链的分布式技术可以让政府部门集中到一个链上，所有办事流程交付智能合约，办事人只要在一个部门通过身份认证以及电子签章，智能合约就可以自动处理并流转，顺序完成后续所有审批和签章。

9、区块链应用场景：公益和慈善

区块链上分布存储的数据的不可篡改性，天然适合用在社会公益场景。

公益流程中的相关信息，如捐赠项目、募集明细、资金流向、受助人反馈等信息，均可以存放在一个特定的区块链上，透明、公开，并通过公示达成社会监督的目的。

10、其他应用场景

【全球首个区块链爱情表达项目】

全球首个区块链爱情表达项目发布，人类首对情侣完成爱情上链表达。“上链的爱是真爱”。

丘比特创始人李晶随后对项目进行了说明和演示，他以“上链的爱是真爱”作为新的爱情共识开始，介绍了丘比特作为全球首个爱情表达的数字权益，是用于爱情表达服务的区块链场景创新应用，用户在丘比特 DAPP 上可以使用各种爱情表达和互动功能，包括爱情上链、真爱见证、爱情矿机、爱的足迹、爱的宣言、爱的分享、暗恋表白、爱的珍藏、爱的收益等各种应用，在各种爱情场景中创造各种体验和权益。

丘比特（CBIT）将“爱情”赋予了实际的意义和价值承载这是一个巨大的场景创新，在爱情共识的场景下，为男女表达爱、传递爱提供了便利，**区块链的不可篡改与爱情的忠贞不渝的属性非常一致，让对爱情此生不移的期待，拥有了精神上的“智能合约”，让爱在链上留存 ，记录生命中最深刻的感动，获得精神上的满足，创造了数字时代的爱情体验，那些敢于上链表达的爱，才是真爱**。

丘比特李晶在现场发布了“丘比特之心“爱情矿机，这是基于窄带物联网 NB-IOT 技术的智能项链，情侣配成一对来使用，当一个人思念另一个人的时候，只要按一下，对方的项链就会震动发光，一句”我想你“就会自动上链表达，记录在链上，并同步会挖矿出来 CBIT，这为那些不善言辞或空间距离比较远的情侣提供了极大的便利和心动的体验，引发了现场的极大兴趣和阵阵掌声。

【加密猫】

加密猫（Crypto Kitties）是一款基于区块链的宠物养成游戏，包括了猫的生育、收集、购买、销售等，也有别称叫云撸猫、云养猫。虽然在互联网历史上有过不少虚拟宠物游戏，但是这个加密猫，可能是人类历史上第一个用户可以永久拥有的虚拟宠物，传统的虚拟宠物是保存在提供服务的公司服务器上的，一旦公司关门歇业，虚拟宠物也就人间蒸发了。

然而，你一旦拥有加密猫，你的所有权会通过智能合约分布式记录在整个互联网上，没法复制，没法销毁，这笔数字资产可以在任何以太坊区块链系统里保存、流通、交易。

加密猫到底有多火爆？自 2017 年 11 月发布以来，加密猫已经聚集了 150 多万用户，交易总价值已经超过 4000 万美元。上线仅几个小时就占据了以太坊超过 15%的网络，贡献了以太币 30%的交易量，直接造成整个以太坊网络的拥堵，可见游戏的热度之高。**有些最热门的猫咪售价竟高达 20 多万美元。从它的销售增速看，每天的成交额能超过 100 多万美元，**

这几乎是半个杀手级应用了。

加密猫到底怎么玩？ 繁殖和收藏是这款游戏的核心玩法。在游戏初始阶段，开发者销售出 100 个创世猫，同时每隔 15 分钟还有一个 0 代猫诞生可以用于买卖。

每只猫长相都不同，基因可以传给下一代：如果让两只电子猫交配，生出的孩子会遗传到各自的 256 个基因组，影响外观、个性、特征等，总计有 40 亿种变化可能。

配种越多次和越晚世代出生的小猫的生育率会下降，越接近第 0 代或外观越独特的猫越贵。

游戏门槛说低不低说高不高，只要你持有以太坊，下载 google chrome 的 MetaMask 插件，然后在 CryptoKitties.co 创建账号即可开玩。

区块链养猫，风险与机会并存。游戏应用和区块链的成功结合，说明了区块链应用进入了一个新的领域。

数字资产保值、增值、变现，取决于稀缺性和后续参与者的人数、热情。我们正赶上一个“消费感受”的时代， 由于“赏玩玩家”的存在，区块链养猫未必是个零和游戏。**加密猫更像是被加密的收藏品，是个人数字财产的一部分，具备唯一性和奢侈品属性**，它们会成为有用户黏性的情感寄托。

不过，目前在国内区块链养猫趣味性不大、缺少社交参与是这个游戏发展的一个瓶颈；但这些痛点的爆发，反过来也会促进区块链游戏应用加速创新，相信在不久的将来，我们能在一个完全个人拥有虚拟资产的世界获得更好的体验。

维基解密将向特朗普总统和希拉里•克林顿国务卿分别赠送两只初代维基加密猫，两只小猫分别以特朗普和克林顿命名，叫作“Trump’s Tender Tabby”和“Clinton Console Kitty” 。

五、结束语

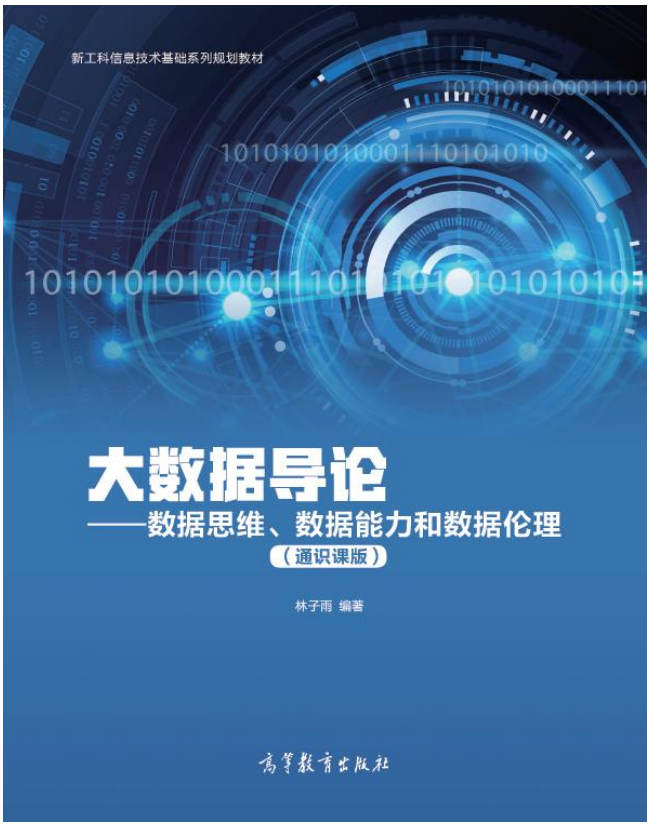
区块链开创了一种在不可信的竞争环境中低成本建立信任的新型计算范式和协作模式，凭借其独有的信任建立机制，实现了穿透式监管和信任逐级传递。区块链源于加密数字货币，目前正在向垂直领域延伸，蕴含着巨大的变革潜力，有望成为数字经济信息基础设施的重要组件，正在改变诸多行业的发展图景。

回顾区块链的发展历程，从最初的加密数字货币走到智能合约，目前继续向更有前景的可编程社会前进，一个个难题被破解，一扇扇门被打开，我们望向远方，激动人心的未来信用社会，正悄悄向我们走进！

附录：厦门大学林子雨编著《大数据导论——数据思维、数据能力和数据伦理（通识课版）》教材介绍

教材官网：http://dblab.xmu.edu.cn/post/bigdataintroduction/

本书详细阐述了培养具有数据素养的综合型人才所需要的大数据相关知识。本书紧紧围绕通识教育核心理念，努力培养学生的数据意识、数据思维、数据伦理和数据能力。全书共 11 章，内容包括大数据概述，大数据与云计算、物联网、人工智能，大数据技术，大数据应用，大数据安全，大数据思维，大数据伦理，数据共享，数据开放，大数据交易，大数据治理。为了避免陷入空洞的理论介绍，本书在很多章节都融入了丰富的案例，这些案例就发生在我们生活的大数据时代，很具有代表性和说服力，能够让学生直观感受相应理论的具体内涵。本书可作为高等学校非计算机专业（尤其是文科）数据科学通识类课程教材，也可供对大数据感兴趣的读者自学使用。


新工科信息技术基础系列规划教材
大数据导论
——数据思维、数据能力和数据伦理
（通识课版）
林子雨 编著
高等教育出版社