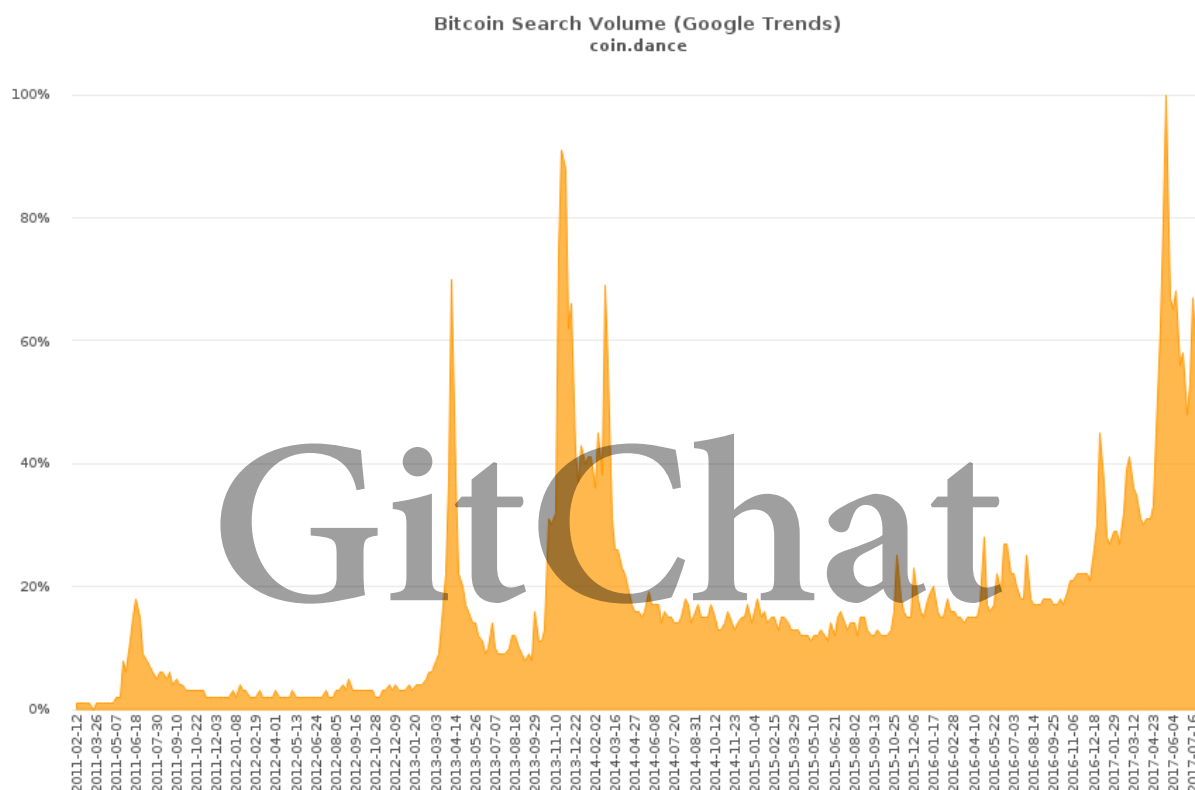
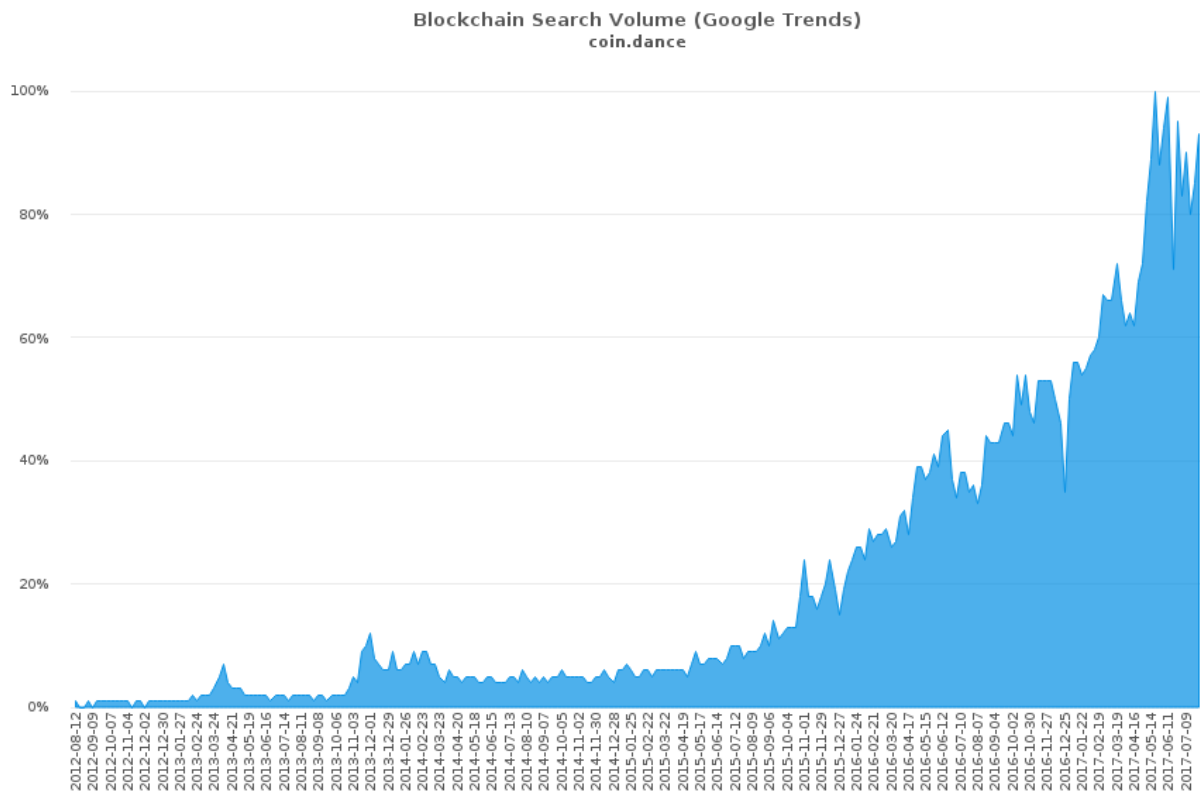


# 比特币和区块链基础

## 专场前言

在全球范围内，比特币和区块链已经成为热潮，有图为证：





当前区块链行业的现状和矛盾是什么？

简单说，现状是冰火两重天。火的一面是，接受并理解区块链的一帮人（姑且称为圈内人），正热火朝天滴向各种行业应用和技术难题进军，融资规模不断刷新（当然这里面鱼龙混杂，后面细说）。冰的一面是，大部分人，包括广大IT人，对区块链认知比较模糊，态度也比较冷淡，质疑和误解的人占了大多数。知识的扩散出现了严重的断层。

冰火两重天的背后有多重原因。第一是因为区块链本身有技术壁垒和理念壁垒，完全理解、真正认同，需要较长的时间。第二，价格波动和投机吸引了圈内人大部分精力，对技术和应用的关注被削弱。在大牛市面前，忙于赚钱的人们没有太多动力去宣传推广。

基于以上考虑，本专题将分享自己几年来对区块链的思考和看法，加速知识扩散，激发关注和创新。我们相信区块链终将颠覆这个世界。

专题着眼点有两个，第一投资，第二创业。换句话说，专题结束时读者的期望收获应是：一，如果我想投资数字货币和区块链，如何判断投资价值，如何思考和分析。第二，如果我要创业，哪些方向值得尝试。

这也是我们标题取为“为什么比特币可以拯救程序猿”的原因。说的更直白点，程序猿至少有四大理由应该关注区块链：

1. 只有程序猿能够深入到代码层。
2. 与其他人相比，程序员们对区块链理解更深刻，投资更可能成功。
3. 区块链能释放出巨大的、无法想象的创新空间。如果你有创业冲动，又有好点子，快来改变世界吧。

4. 巨大的认知快感：还能这么玩啊，为啥我没有想到。

强烈建议大家研究区块链，积极地投资或创业，机会实在是太多，不论是金钱上的还是事业上的。你们拥有巨大的优势，面临巨大的机遇。真心羡慕你们，作为一个代码白痴，丹华只能为大家摇旗呐喊，期待未来能在各位的独角兽公司里谋个一官半职。

## 01-比特币和区块链基础

本场chat是系列第一场，介绍比特币、区块链和数字货币的基础知识。比特币和区块链是技术进步的产物，本身有一定的技术门槛。本节将采用简单易懂的方式介绍基本原理，为后续的话题深入做准备。具体包括：

- 开场: 减半发行是个什么鬼？
- 比特币的基本结构。
- 为什么比特币这么牛？
- 挖矿与矿池格局。
- 为什么区块链不可更改？
- 智能合约。
- 币众筹ICO。

### 减半发行是个什么鬼

以一个高中数学题开场。

假设有一个数列，第一个数字是1，第二个数字是0.5，第三个是0.25，每一项是前一项的一半，无穷列下去。问数列的总和是多少？

简单心算下，结果是2。数列总和是第一项的2倍。比特币总发行量是2100万个,来源就在这里。

2018年高考数学压轴题

比特币软件设定：每10分钟产生一个区块，初始四年里，矿工每发现一个新区块的奖励（新发行币）为50个比特币，以后区块奖励每四年减半（或准确说是每隔210,000个块），即后续四年每一个区块新发行25个比特币，再过四年一个区块新发行12.5个比特币，以此类推。

问：比特币发行总量是多少？

解答：

第一个四年挖掘的比特币总量为： $A=50*6*24*365*4=10512000$ 个。

套上面公式，最终挖出来的比特币总量就是第一个四年的2倍，2100万个。当前已经进入第三个四年，也即是说，75%的比特币已经被挖出来，在市场上流通。

当前的区块奖励是12.5个。换句话说，假设读完本文需要20分钟，则在这20分钟里，比特币网络会产生2个区块，对应新发行25个比特币，合计约75万元人民币价值。全世界的矿工，在这20分钟内，抢夺这75万元的收益。

## 比特币的诞生

比特币的诞生要从2008年说起。

当时，全球深陷金融危机，人们普遍对大型金融机构失去了信心，甚至包括技术专家。有一个自称为中本聪的匿名人士——我们现在还不知道他到底是谁——在网上公开了一篇文章，提出了比特币的理论构想。次年1月，比特币软件诞生，创世区块被挖出，从此打开了数字货币创新的潘多拉盒子。

非常有意思的是，中本聪在创世区块里留下一句不可修改的话：

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

翻译过来：2009年1月3日，泰晤士报头条——财政大臣正处于对银行实施第二轮紧急援助的边缘）。

这句话，也许意味着中本聪对于传统金融的嘲弄。

比特币的设计本身，蕴含着无政府主义（去中心化）和技术理想主义（严格限定的区块生成与新币发行机制）的色彩。整个体系透露出了对政府和金融机构强烈的不信任，也被激进人士解读为对通胀型法币的反抗和不信任。

所以，比特币的内在是有价值观偏好的。

## 比特币的基本结构

比特币的基本结构可以用以下9段话概述：

1. 比特币有三重含义：既代表比特币网络，也指网络节点使用的比特币软件，也可以指网络中交易的数字货币单位（Token）。
2. 比特币网络是一个由若干节点组成的用以广播交易信息和数据区块的P2P网络，这个网络包括矿工、比特币软件、钱包、用户、交易所等。
3. 矿工指通过不断重复哈希运算来产生工作量证明的各网络节点。矿工主要负责验证交易，并将交易打包成区块，获得区块奖励和交易手续费（也称矿工费）作为回报。

4. 比特币软件是系统的核心软件，目前比特币软件的开发由Bitcoin Core团队完成，也有一些竞争团队。对核心软件的改进协议被称为BIP。
5. 钱包指保存比特币地址和私钥的软件，可以用它来接受、发送、储存你的比特币。用户应保管好自己的钱包，防止丢失私钥。

比特币网络中，人们用比特币地址来接收和管理比特币，类似于邮件地址。地址看起来像一串乱码，因为长这样：19fJnPC4vsvXFkx77TB95GFLnMVKoTo45v，特征是以阿拉伯数字“1”开头。

6. 处理交易是比特币网络的核心功能。一笔交易是指把比特币从一个地址转到另一个地址。更精确地，一笔“交易”指一个经过签名运算的、表达价值转移的数据结构。每一笔“交易”都经过比特币网络广播和传输，由矿工节点收集并封包至区块中，永久保存在区块链某处。
7. 区块和区块链：一个区块就是若干交易数据的集合，它会被标记上时间戳和之前一个区块的独特标记。区块头经过哈希运算后会生成一份工作量证明，从而验证区块中的交易。有效的区块经过全网络的共识后会被追加到主区块链中。
8. 比特币代表了数十年的密码学和分布式系统的巅峰之作，这是一个独特而强大的组合，汇集了四个关键的创新点。包括：

一个去中心化的点对点网络（比特币协议）

一个公共的交易账簿（区块链）

一个去中心化的数学的和确定性的货币发行（分布式挖矿）

一个去中心化的交易验证系统（交易脚本）

这四点紧密协作，形成了整个比特币的软件系统。

9. 交易所是指提供数字货币与法币兑换平台的公司，是比特币生态系统的重要环节。交易所本身与比特币网络无关，可以将交易所理解为比特币网络的企业用户。目前多数用户买卖比特币是通过交易所来完成的（也可以选择线下交易）。目前全球有几千家交易所公司，国内也有几十家，均为小型创业公司，规模不一。

## 为什么比特币这么牛？

为什么说比特币的设计很牛逼呢？解释一下你就懂了。

当前互联网主要是信息传递，从早期的公告板到现在的微信Facebook，已经能实现全世界任意两点可以非常便捷地传递信息。但是，任意两点的转账现在还无法实现。国内支付宝和微信支付实现全国范围的自由转账，但是在全球范围，依然需要依赖传统金融体系。

比特币的牛逼之处就在于，它第一次实现了任何人可以在任何地方将价值即时地（instantly）传输给地球上另外一个人，而不需要任何中介。人们称以比特币为代表的互联网为“价值互联网”，以区别于当前的所谓信息互联网。

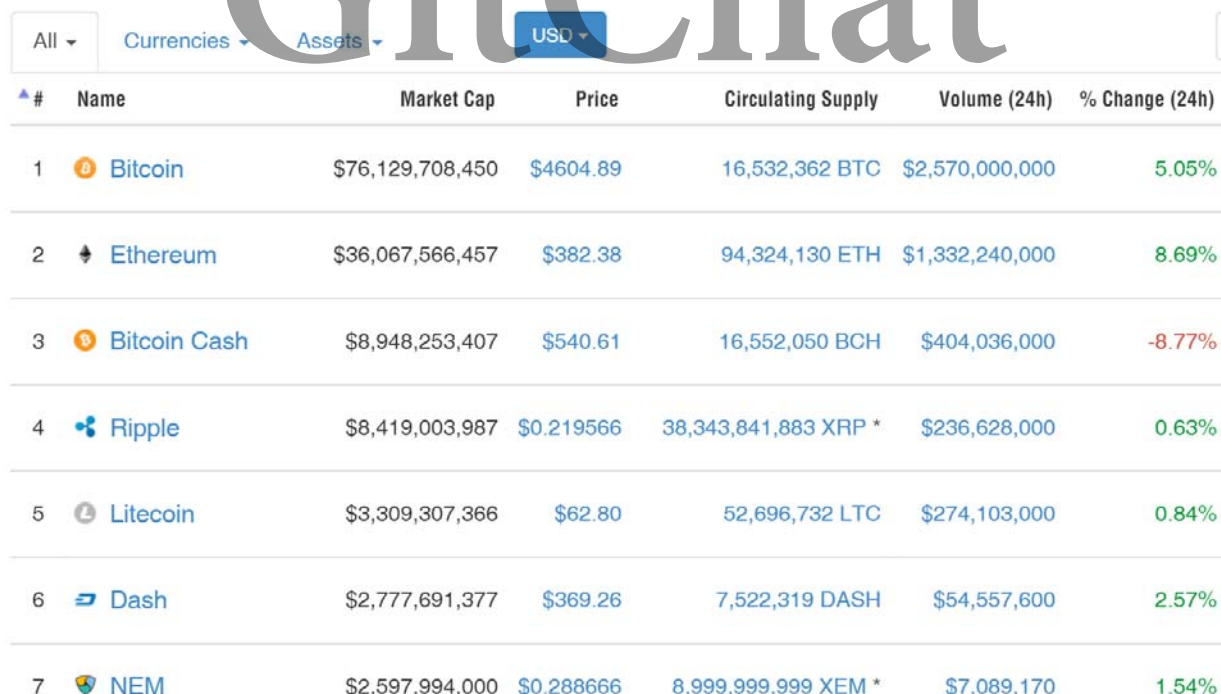
比特币采用P2P网络结构，极度扁平化，没有中央权威，也没有负责流通记账的银行体系。系统通过比特币网络中的众多节点（矿工）来管理交易、发行新货币。它是开源的、公开的、透明的，任何人都可以参与其中。没有任何个人或单一实体能够完全控制比特币系统。

比特币诞生后，人们被其设计上的简洁优美和激发的无穷可能性震惊，开始疯狂地投资或复制它，进而衍生出了无数的“仿制版本”，一般称之为山寨币。有些山寨币是对比特币的简单模仿和参数修改，有些则具有颠覆性。

至此，数字货币行业正式出现在历史舞台上。

所谓数字货币，也称加密货币，一般是指内含区块链技术（Blockchain）的去中心化网络中的内生交易代币。典型的数字货币包括比特币、以太坊、莱特币等，也包括一些分叉币，比如以太坊经典、Bitcoin Cash（BCC）等。比特币是其中第一个、也是最成功、市值规模最大的数字货币品种。

目前世界上一共有800多种数字货币，行业总市值达到1600亿美元。如果要浏览目前所有的数字货币品种，推荐网站[www.coinmarketcap.com](http://www.coinmarketcap.com)。下图列出了市值排序的前7大数字货币。

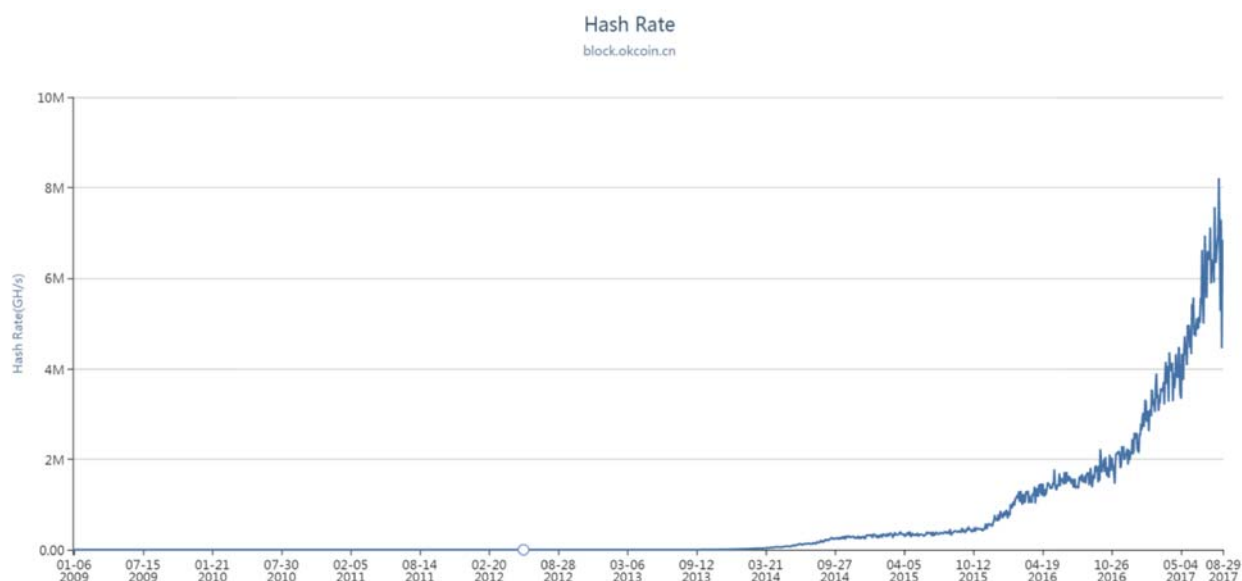


#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)
1	Bitcoin	\$76,129,708,450	\$4604.89	16,532,362 BTC	\$2,570,000,000	5.05%
2	Ethereum	\$36,067,566,457	\$382.38	94,324,130 ETH	\$1,332,240,000	8.69%
3	Bitcoin Cash	\$8,948,253,407	\$540.61	16,552,050 BCH	\$404,036,000	-8.77%
4	Ripple	\$8,419,003,987	\$0.219566	38,343,841,883 XRP *	\$236,628,000	0.63%
5	Litecoin	\$3,309,307,366	\$62.80	52,696,732 LTC	\$274,103,000	0.84%
6	Dash	\$2,777,691,377	\$369.26	7,522,319 DASH	\$54,557,600	2.57%
7	NEM	\$2,597,994,000	\$0.288666	8,999,999,999 XEM *	\$7,089,170	1.54%

## 挖矿与矿池格局

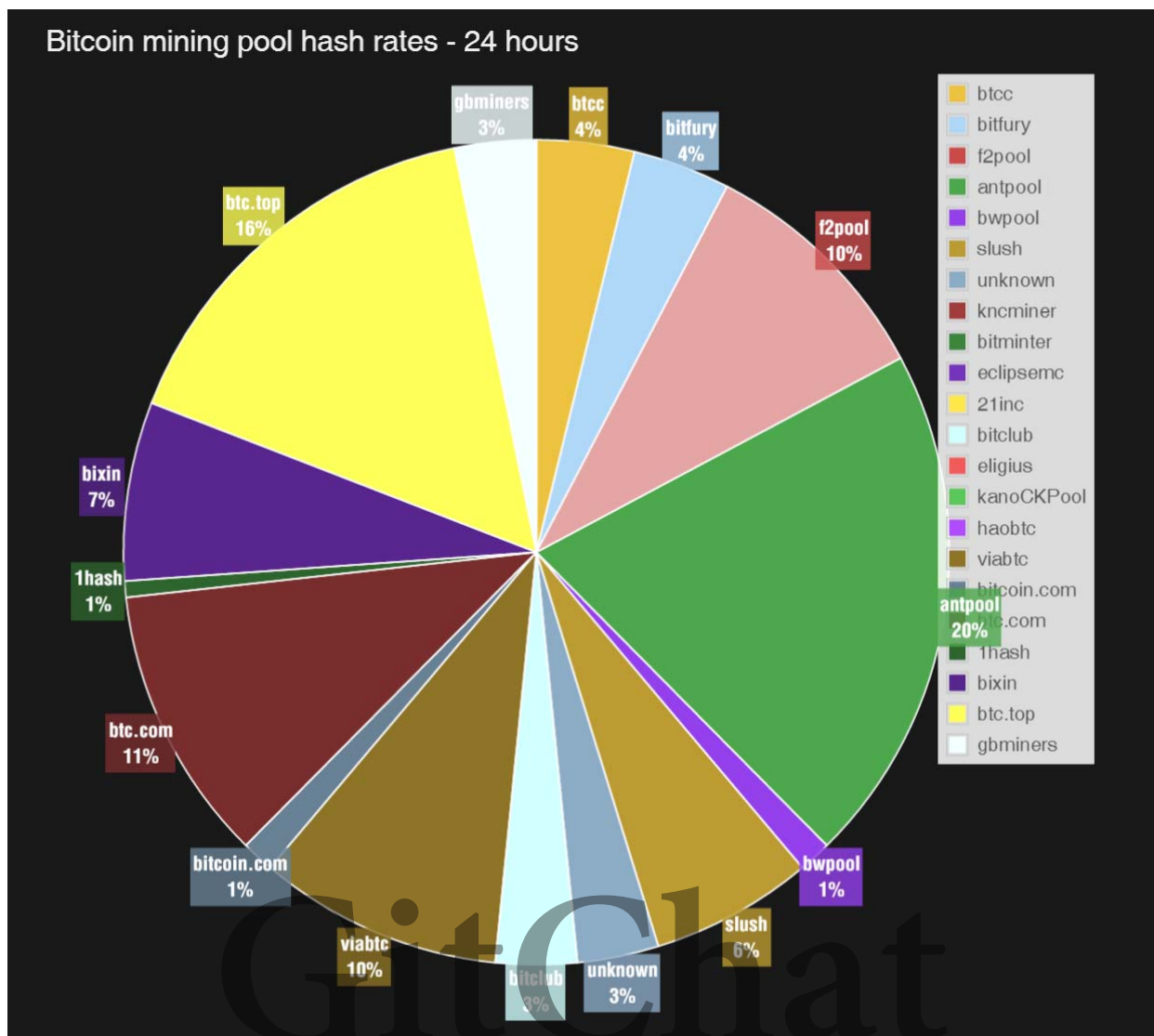
庞大的去中心化网络中，有个人和企业节点，也有专门从事挖矿的矿工。他们拥有巨大的机房，这些机器负责验证网络中发生的所有交易，并将其打包成一个个区块（10分钟一个），这些区块通过hash算法串联成区块链。

所有矿工汇集的庞大算力，实质上构成了对比特币网络的一种物理保护。因为，要篡改网络数据或攻击整个网络，需要付出巨大的算力成本。又因为网络是去中心化的，局部的瘫痪不影响全网运行。节点越多，算力越高，网络安全性越高。下图显示为比特币诞生以来网络算力的变化趋势图。



矿工们做这些，当然不会免费。网络给矿工的回报是，挖出新区块的矿工将得到区块奖励Coinbase和区块中每笔交易固有的交易费。最早的区块奖励是50个比特币，之后缩减到25个，当前是12.5个。

新币发行数量虽然减少到四分之一，但价格翻了远远不止4倍，上千倍了，所以依然有无数人杀进来。**比特币算力和价格已经构成了正反馈环，算力竞争已经实质上变成了一场残酷的军备竞赛。**目前的矿池格局基本稳定，主要由中国和美国的玩家组成,大矿池包括 antpool、btc.top、f2pool、btc.com、viabtc.com等。如下图所示：



为什么区块链不可更改？

人们经常说，区块链的交易记录是不可更改的，是可信的。为什么？

理解这点需要引入一个概念：Hash算法。Hash算法有很多种，基本功能是：将任意长度的数据文件转换成一个唯一对应的固定长度字符串。你可以理解为，给任意一个文件生成了一串固定长度的乱码一样的标签。这个算法是不可逆的，就是说，你拿到这个标签，无法反向推导出原来的数据文件。如果数据文件有一点点变动，比如加了个标点符号，那么重新hash之后，新的标签也与原标签大不相同。无法从新旧标签的差异推测数据文件发生了什么变化。因此，通过标签，可以很容易地验证某个文件在某个时刻是存在的，或者验证两个文件是否相同。

正是这种不可逆性，决定了区块链的不可更改性。每个区块中，除了十分钟内的转账交易数据之外，还有一个区块头。区块头包含了对上一个区块数据的hash值。这些hash层层嵌套，长度固定，最终将所有区块串联起来，形成区块链。区块链里包含了自该链诞生以来发生的所有交易和所有新币发行。

假如我是坏人，我要篡改一笔交易。交易包括发送方和接收方，以及转账的数量。发送方的比特币可以一路追溯到最早新发行该币的区块。发送方拥有这些比特币的合法性，是由该币的原始发行区块记录和该币有关的所有历史交易记录保证的。因此，要篡改一



笔交易，意味着它之后的所有hash和相关交易记录全部要篡改一遍，这需要的算力和难度极高，成功概率为零。

所以有所谓6个确认的问题。一笔交易被打包成区块后，再串接6个区块，这个交易才是基本无法更改的。可以类比排队。如果所有人都认可最长的队伍是合法的队伍，那么你排上之后，最关心的应该是：有多少人排在你后面。因为，排在你后面的人越多，你的合法利益越稳固。

新闻上经常用铁索链条图片来展示区块链，严格来说，这是不准确的。铁链或者项链，结构都是线性的。去掉其中一环，整个链条损失不大。区块链的结构不是这样，因为有hash算法，咬合的更加坚固，无法改动一点而不伤及其他。这就是区块链不可更改特性的源泉。

。

## 区块链的应用前景

理解了这些，再对照传统的金融系统，就知道：为啥区块链初听起来这么古怪难以理解，但是一旦理解之后，就会立马惊呼：卧槽，这才是未来，这才是金融的未来。什么P2P借贷、互联网金融，都是渣渣中的渣渣。

首先，数字货币有纯正的互联网基因。当前的各种互联网金融尝试，大多依附于传统金融体系，变革不够彻底，先天不足。

其次，它首次实现“技术驱动金融”。传统金融里，技术由IT部门负责，业务部门提需求，IT负责实施。比特币不同，它由技术天才制定了一套完整的游戏规则，主导了系统的运行和发展。这是基本范式的巨大转变。

这一点的后果就是，未来的金融创新是由金融思维的技术天才主导，银行家们只能干瞪眼。

第三，作为货币形式，与黄金和纸币相比，它有一系列的优势：体积小，稀缺性高，价值大，容易分割，质量均匀，不会腐烂变质，便于携带，难以伪造，透明度高，可追溯可审计，去中心化（发行流通结算簿记等内生地整合在一起），低门槛（任何人可以接入），低成本，无国界，可编程性。当然了，缺点也是很明显的，比如交易不可撤回，耗电，币值不稳定等。

第四，去中心化的区块链本质上是一个永不停息的机器，这开启了大规模、分布式协作的典范。利用这种模式，我们可以做很多之前无法想象的事情。未来在区块链的驱动下，我们不再局限于一种职业一个公司，随时可以参与到自己感兴趣的项目中去（即使它远在地球另一端），贡献自己的力量，并获得对应回报。

第五，比特币将释放一个更大的世界。且让我们拾级而上。

如果将比特币理解为货币和支付网络，从人类早期的以物易物，到贝壳、金属货币、黄金白银、纸币，到现在的无现金网络（支付宝等），到比特币为代表的数字货币，你会发现，这是一个自然的升级过程：**货币一步步虚拟化，一步步脱离我们对于实物和实体**

**的信任。**金融系统变得越来越无信任、自我信任。比特币只不过是将其最本质、最不可或缺的因素抽象出来了，剥离了物理和人的因素。

认为比特币没有价值的人，多数是沉溺在“实物信任”和“实体信任”的固有框架中，没有意识到，在货币演化的漫长历史中，人们对于实物和实体固有的信任成分越来越弱。

之前我们信任黄金，信任国王/皇帝，后来我们信任美元（美元上刻有In God we Trust），信任政府和银行。未来，我们将彻底脱离了金融中介，信任区块链，信任数学和代码。

让我们抽象一点。

比特币网络的核心是处理交易，而且是最简单的交易。能不能扩展一下，做一些复杂的交易呢？比如债券、股票、房地产、任何其他资产和权利？

当然可以。

了解固定收益业务的朋友，都会对债券交易（多市场、多环节等）心生恐惧，一个环节出问题就能让你生不如死。

买过房子的人，也都能体会房产交易的痛苦。假如产权证书都是电子化的，交易各方采用多重签名，交易流程将大大简化。

还有证券、保险这些业务，都可以尝试区块链。具体的应用模式我们将在后续文章中深入讨论。

类似的还有知识产权（IP）市场。听音乐、看视频，都可以做成一次交易，即使交易额很小。由于数字货币可以无限细分，因此天然滴适合小额交易。可以想象，这将释放海量的长尾市场。

## 智能合约

这些交易还是太简单，能不能再抽象一点呢？

最复杂最抽象的交易是什么？

是合同。

合同代表了不信任或者弱信任的双方做交易的标准形式。人们之所以信任合同、尊重合同，因为背后的机制是法律、律师、法庭、文化和道德感。技术天才们已经雄心勃勃，要把合同——这一最复杂的交易形式，也搬到区块链上。这就是所谓智能合约smart contract，以编程和自动执行的方式来执行合约，实践“代码即法律”的理念，完全杜绝了合同执行中的认定不同、扯皮推诿和诉讼的情况。

牛逼闪闪的以太坊，就是立志成为一个通用的、图灵完备的智能合约平台。其内生代币以太币，成为执行智能合约的“燃料”。矿工每执行一步智能合约的代码，需要获得一定的以太币作为激励。

这个角度上说，智能合约的抽象层次更高，所以市场前景更大。

数字货币和区块链，不仅仅是个软件发明，更是社会基本模式的转变。它的扩散和演化可能深刻地改变世界运行的方式，甚至人类社会的理念-共同想象（共识）。

## 币众筹ICO

首次代币发行（Initial Coin Offering，ICO），类似于股票上市的IPO。ICO是一种众筹方式，你给我钱（人民币、比特币、以太币等），我给你一定比例的项目代币。它是法律监管之外的、不依赖主流融资渠道的草根融资形式，今年持续火爆。

投资者拿到的代币是什么性质，具体取决于项目本身的设定。多数代币是针对某一区块链项目，该代币是链上的流通资产。项目团队利用该链实现某些特定的应用，激励更多的参与者购买、使用、交易这些代币，实现代币的升值和货币化。也有一些代币，本身规定了项目的收益权、分红权、投票权（类似股票）。跟IPO不同的是，IPO都是成熟公司，而ICO往往本身就是一个初步想法（用白皮书披露），一个团队，就可以公开宣称自己开始ICO。所以，ICO融资对应于股权投资中的种子轮融资，非常早期，风险也较大。

ICO不像IPO有股权和所有权特征，多数投资者看中的是上市后的增值，类似于打新股获得的一二级市场差价和炒作价值。IPO的要求很高，流程很慢，而ICO没有任何门槛，速度很快，容易跨国境，适合小项目和全球项目。

ICO的缺陷也很明显，信息披露、反洗钱、投资者保护、投资者适当性管理也严重不到位。

最早的ICO是在2013年，万事达币，募集了5000多个比特币，最后失败了。最成功的ICO'是以太坊，当时募集了1800万美元的比特币，现在以太坊市值270亿美元。

2017年是ICO爆发的元年，诞生了无数的过亿项目，市值上涨有几倍几十倍几百倍的都有。国内截止到7月中旬，有大概26亿元的ICO项目。

大多数项目，在ICO结束后，会寻求让新的项目代币到某个交易平台上线交易，就是能够兑换法币。这就相当于二级市场。

如何判断一个ICO项目好不好？

答案——基本靠猜。因为你能拿到的信息非常有限。实在要评估，就按照VC的思路来，看看项目团队靠不靠谱，看看项目内容是不是合乎逻辑，等等。当然并不是所有项目都能找到交易所，顺利卖掉。如果不能在交易所上市，只能私下交易。

ICO当然面临着法律监管的风险，一旦政府宣布ICO非法，代币价格将可能暴跌，市场热度也会迅速下降。另外，目前ICO市场鱼龙混杂，必然有很多诈骗、圈钱的项目，甚至圈钱跑路的项目。因此，项目团队跑路也是不得不防的。在我们成文的这几天，中国已经开始对ICO实施监管，一些平台和会议被叫停，有新闻称ICO涉嫌非法集资。

还有一个风险，ICO平台风险。撮合方也有可能倒闭或者跑路，或者遭遇法律风险。

美国SEC已经就ICO的风险发出数次警告，认为“ICO”和“Token Sales”(代币销售)依然受到联邦证券法律的监管。随后，交易所Bitfinex宣布将不再为美国投资者提供该交易平台上线的部分ICO代币，同时还将对其他相关服务进行整改。

8月24日，国务院法制办发文称，由中国银监会起草的《处置非法集资条例》在中国政府法制信息网公开征求意见。8月30日晚间,中国互联网金融协会发布《关于防范各类以ICO名义吸收投资相关风险的提示》(以下简称“风险提示”),称部分机构以ICO为名义从事融资活动,相关金融活动未获得任何许可,其中涉嫌诈骗、非法证券、非法集资等行为，提醒广大投资人提高警惕，谨慎的对待，自行承担投资风险。

相信，未来对于ICO的监管政策一定会出台，是一刀切，还是沙盒，还是宽松的备案制，拭目以待。（全文完）

# GitChat