本篇文章给大家谈谈区块链，以及区块链与博弈论对应的知识点，文章可能有点长，但是希望大家可以阅读完，增长自己的知识，最重要的是希望对各位有所帮助，可以解决了您的问题，不要忘了收藏本站喔。

本文目录

区块链有什么作用？

本文整合一年前区块链兴起时很火的以第一人称陈述的通俗易懂的说法。

大家好，我就是神秘的区块链，要想了解我，那就要先从我的族谱说起：

区块链的父亲：去中心化

我父亲出生在全人类的一个虚拟世界里，是生活在全人类脑中的一个信仰。在英语里面，我们把他称为Decentralization。在中文世界，他也给自己取了个时髦的名字，叫去中心化。但在互联网上，人们习惯叫他P2P。

我父亲在人类出现的时候就已经存在了，他是去掉中心，然后实现人与人之间直接沟通、直接交易、直接传播的一种方式的信仰。他相信总有一天，我们可能不再需要中心化的机构。

在人类几十万年的历史中间，父亲一直都在寻找一位能实现他去中心化哲学理想，并且他真正爱的人。

他喜欢过很多各种各样的人，但直到我母亲的出现，他才意识到什么是真爱。

区块链的母亲：互联网

我的母亲，就是互联网。

互联网是一个没有中心化节点的网络结构。每一个点，从本质上来说，在整个互联网上都是同等重要的存在。所以我的父亲自从遇到母亲之后，就彻底地疯狂地爱上了她。然后他们俩就结合，组成了家庭。

之后，他们生下了延续父亲去中心化基因，并且对整个世界产生巨大影响的8个孩子。

我排行老七，前面有6个哥哥姐姐，后面还有1个弟弟，这就是我的家族。下面请允许我给大家介绍几个我的兄弟姐妹。

大哥：P2P下载

我的大哥，他的名字叫做P2P下载。P2P是我父亲的姓氏，所以第一个孩子姓P2P，名字叫下载。

大哥是在1999年来到这个世界的，帮他接生的，是今天互联网界非常著名的一个创业者，他的名字叫ShawnFanning。他1999年创立了一个叫Napster的mp3音乐分享网站，他也是Facebook最早的顾问、投资人和股东之一。

Napster，能让大家自由下载MP3，但是这个mp3文件，并不是放在Napster网站的硬盘上的。如果是这样的话，把整个互联网上的音乐都放在这儿，存储量是非常大的。

于是Shawn做了一件事，就是将每个人电脑上的mp3汇集成一张目录。如果你想下载mp3，那么Napster就会找到那些有这个mp3的电脑，同时去从这些电脑中下载一个个小小的碎片，然后在你的电脑上拼成这个mp3。所以Napster本身并不拥有MP3，他只是帮助那些拥有mp3的人互相分享，我们把这个叫做点对点的分享。

后来，大哥在中国也有了一个对应的形态，就是迅雷。迅雷就是做P2P下载的，它的逻辑是把电影文件，放到每个不同的电脑上，然后彼此分享，这个模式极大地节省了资源。

我的父母非常高兴，因为大哥为人类带来了很大的改变。当然这也不是一帆风顺的，因为P2P下载对版权保护的冲击很大，美国后来禁止用这种方式来分享MP3，Napster也于2002年宣告破产。

但是这个逻辑，一直存续了下来。

我的二哥：CDN

我的父母，接着生下了他们第二个孩子，也就是我的二哥——CDN。

当时，大家在互联网上看电影，有一个问题。比如你在上海通过视频网站看一部电

影，因为电影是存放在北京的服务器上，在上海看就会很慢，如果在深圳去看这个电影，反应会更慢。

那怎么办？有一个办法就是把这个电影放在很多不同地区的服务器，看电影时找最近的服务器来访问，这就是CDN。

于是，美国和中国的很多电信公司，就成了我二哥的接生婆。他们把内容放在很多不同的地方。你在上海看电影，就从离你最近的机房——上海的服务器上看。在北京看电影的人，是在北京服务器上看。这是一种分布式的存储，共享分布式的带宽。

过去我们把内容放在机房，无论在中国还是美国，机房的数量都是有限的。如果能够把每个人家里的带宽，都拿出来，这样你看电影时，访问的是你邻居家的电脑，速度是最快的。

关于P-CDN的落地，我们还要感谢帮大哥在中国落地生根的那家公司——迅雷。迅雷很早就开始用P-CDN，它出售给会员一种商品，当年叫赚钱宝，后来叫玩客币，其实都是让会员用家里面的网络，来访问彼此网络带宽的一种设备。

除了迅雷，我们还要感谢那些电信机房，感谢Shawn，感谢Napster，让大哥分享硬盘、二哥分享网络资源这样的方式能够出生和成长。

我的三哥：分布式计算

接着我的第三个哥哥出生了，他的名字叫做分布式计算。三哥是个科学家，他出生的时候，轰动了全世界。

我三哥在做什么事呢？

过去我们破译一个算法或者密码，我们用一个东西：超级计算机。就是在机房里有个特别厉害的计算机，它的运算速度，比全世界任何一台计算机都要快。这就是中心化的计算。

那什么叫做分布式计算呢？就把需要大量计算的工作，比如说，破译密码，或者计算一个DNA的序列，分解成无数的小块。分成小块后，再扔给全世界一个个小的计算机，比如你家里的个人电脑。

当全世界几千，几万甚至几十万台个人电脑的CPU，同时计算的时候，再怎么样，计算速度都会比一个超级计算机要快。

我的四姐：社交媒体

在这之后，我的父母生了我四姐——社交媒体，她是我的父母生下来的第一个女孩，所以他们特别喜欢她。

过去媒体是中心化的，虽然它有可能代表正义，有可能代表一个中立的观点，在全世界范围之内，发言权是集中在少数人手上的。

我的四姐诞生后，她让每个人都有公平发言的机会，每个人的声音都能被别人听到，整个世界就立刻变得非常感性，每个人都能够说出自己有创意的、有感情的想法。

谁是把我四姐接生下来的人呢？在美国我们特别要感谢Facebook、Twitter，在中国我们要感谢新浪微博和腾讯，是他们共同把四姐接生下来。

四姐的出生让我的父母信心大增，是她让每个人的声音都可以被全世界听到，她是互联网世界，人人都喜爱的一朵鲜花。

我的五哥：P2P借贷

我的父母突然想到，能不能在金融领域，也生个孩子呢？他们借助一个叫雷纳德·拉普兰奇的美国人，把五哥接生下来，给他取名叫P2P借贷。

P2P借贷是什么意思呢？就是今天我需要钱，我不去银行，而是直接去找有钱人借。

在美国，你今天到银行存钱，活期的储蓄利率是一年0.25%，可是如果去借钱刷信用卡的话，那信用卡的利率一年17%。凭什么把钱存银行是0.25%，把钱取出来就17%呢，这太没道理了！那还不如去中心化，直接把钱借给对方。

这就是我的五哥P2P借贷，他是一个非常叛逆的孩子。他一直在宣扬人与人之间是可以直接发生借贷的，所以跟传统世界一个特别顽固和保守的群体，发生了很大的抗争。五哥在全世界做了很多他人觉得风险很大的事情，但也帮助很多人借到了钱。

我的六哥：众筹

我的父母在金融领域生下我的五哥之后，很快又生下了六哥，他叫众筹，帮他接生的是一个美国的公司，名字叫做Angellist，天使列表的意思。

今天的金融世界里是有监管的，因为世界上有很多不合格的投资人，就是那些对风险没有识别能力和承受能力的人，拿他们的钱，会有金融风险。

在中国超过200人叫非法集资，我们能不能在200人之内，找到对风险有识别能力和承受能力的人，拿他们的钱，而不需要通过中间机构呢？我们把这种方式叫做众筹，这就是我的六哥。

与我的五哥相比，六哥会显得稍微沉稳一点。但他依然会让全世界觉得头疼，因为还是涉及到金融风险。但是他让很多优秀的创业者拿到了投资，让他们能够有机会去改变这个世界。

美国打车软件Uber，这家在全世界引起巨大反响的公司，他们的第一笔钱，就是从angellist通过众筹的方式拿到的。

我，小七：区块链

我是第七个孩子，我叫做区块链，帮我接生的人叫做中本聪。中本聪在2008年发表了一篇论文，这篇论文的标题叫做《基于点对点技术的数字现金系统》。

我想跟大家强调两点，第一是基于点对点技术，点对点就是我的父亲，也就是P2P。

第二个叫做数字现金，

什么是现金？纸币、黄金、白银都是现金。所以我是来做黄金的，做纸币的，不是来做银行账户的。

怎么去实现它呢？就是用我的父亲的基因——点对点技术，把这个记账的能力，放在每一台电脑上。

我是一种基于分布式的记账技术，我天生有分布式记账的优势，但是我身上也有些缺陷，我不能解决所有问题。

我的缺陷是什么？分布式记账，意味着过去一个银行要记的账本，现在需要存储在全网的每个节点上。而要在每台电脑上存储的时候，就造成了极大的资源浪费。你们可能没有意识到，但我自己其实深受其苦。

所以我只能在数据量特别小的领域，来做分布式记账，数据量特别大的领域我干不了。比如说很多人期待我能做大哥做的事情，就是把文件在全网来分享。但是在全

网每个节点上放个副本，需要消耗极大的资源。

分布式记账最大的作用就是去除中间的信任机构。在我的努力之下，一些第三方的信用机构将来可能不再被需要，人类生活的效率将得到提高。

对于区块链技术的研究需要做好哪些准备工作

我建议你在深入研究之前，先加强对基本原理的理解。区块链建立在计算机科学、密码学和经济学数十年研究的基础上。中本聪是一个“反叛者”，但他也很清楚之前的历史。为了理解区块链的工作原理，您需要了解先于区块链产生的区块，以及为什么他们不起作用。

以下是一些需要熟悉的预备知识，按重要性排序。（注意，以下内容里的链接只是一个学习起点，您可能会想深入了解更多。）

计算机科学

数据结构

您需要熟悉主要数据结构的特性和复杂性保证：linkedlists,binarysearchtrees,hashmaps,以及graphs（特别是在区块链中具有显著特征的有向非循环图）。从头开始构建它们有助于更好地理解它们的工作方式和属性。

密码学

密码学是加密货币的代名词和基础。所有加密货币都使用公钥/私钥加密（public/privatekeycryptography）作为身份和身份验证的基础。我建议学习RSA（RSA）（它很容易学习，不需要很强的数学背景），然后看看ecdsa（ECDSA）。椭圆曲线密码需要更抽象的数学——理解所有细节并不重要，但要知道，这是大多数加密货币（包括比特币）使用的密码。

另一个重要的密码原语是密码散列函数（哈希函数）。这些可用于承诺机制，并且是merkle树的构建块。Merkletrees支持Merkleproofs，这是区块链用于可扩展性的关键优化之一。

分布式系统

关于分布式系统有一些很好的教科书，但这是一个庞大而困难的研究领域。分布式系统对于区块链的论证是绝对必要的，因此在处理区块链编程之前必须在此建立基

础。

一旦你的系统不再运行在一台机器上，就必须开始论证一致性和共识。您需要了解可线性化和最终一致性模型之间的区别。您还需要了解容错一致性算法的保证，例如Paxos和RAFT。了解在分布式系统中论证时间的困难，理解安全与活性之间的权衡。

有了这样的背景，你将能够理解拜占庭容错共识的难点，这是公共区块链的主要安全要求。您将需要了解PBFT，这是首个提供拜占庭容错共识的可扩展算法之一。PBFT是许多非工作证明区块链一致性算法的基础。再次提醒，你不需要了解PBFT太多的细节，而是总体的思路及其安全性保障机制。

理解传统的分布式数据库也是非常有用的（其核心思想是，区块链本质上是数据库）。了解分片（例如通过一致性哈希），主从复制（leader-followerreplication），分布式哈希表(DHTs)，例如Chord或Kademlia。

网络

区块链的分布式在很大程度上源于其点对点网络拓扑结构。因此，区块链是过去p2p网络的直接产物。

要了解区块链通信模型，您需要了解计算机网络的基础知识：如TCP与UDP、数据包模型、IP数据包，以及大致的网络路由工作方式。

公共区块链倾向于通过gossipprotocols和flooding来传播信息。学习p2p网络设计的历史，包括NapstertoGnutella,BitTorrent，Tor，都具有一定的指导意义。区块链有自己的特点，但它们借鉴了这些网络的经验教训以及它们是如何设计的。

经济学

加密货币本质上是多学科的-这是使它们如此迷人和激进的主要原因。除了计算机科学，密码学和网络，它们还与经济学密切相关。加密货币可以通过其经济结构获得许多安全属性，这通常被称为加密经济学。因此，经济学对于理解加密货币至关重要。

博弈论

对加密货币最重要的经济学分支是博弈论，即研究多个主体之间的收益和激励。你不需要深入到很细节，但你需要了解博弈论分析的基本工具，以及如何使用它们来

分析一次性和持续性游戏中的激励因素。

你需要掌握两个关键的概念：纳什均衡点和谢林点，因为它们在密码学分析中具有突出的特点。

宏观经济学

加密货币不仅是协议，也是货币的形式。因此，它们响应宏观经济规律（如果它们可以被称为规律的话）。加密货币受制于不同的货币政策，并对通货膨胀和通货紧缩作出可预见的反应。你应该了解这些过程以及它们对支出、储蓄等的影响。

另一个有价值的经济概念是货币的流通速度，特别是当它与货币的价值相对应时。

微观经济学

加密货币也深深地与市场交织在一起，这需要了解微观经济学。你需要对供求曲线有很强的直觉。你应该能够解释竞争和机会成本（它们将经常应用于挖矿领域）。在许多硬币发行和密码经济系统中，拍卖理论具有突出的特点。

我希望你已经熟悉了其中的一些话题。如果是的话，请随意浏览或跳过它们。

好吧，到现在为止，你已经完成并巩固了你的基础知识，现在您已经掌握了以上的理论，让我们来开始区块链开发吧。

比特币、以太坊、区块链、代币、ICO，分别是什么意思？

数字货币在去年掀起了轩然大波，百倍币、千倍币层出不穷，一茬一茬信仰者、投机分子以姿态各异的面目参与其中，实现了财富自由。无数人为之癫狂，数字货币成为了一种即使你认为是一个骗局，也无法忽视的存在。而这一切的一切的开端，要从化名中本聪，至今仍然大隐于世，无人知其身份的天才发表的论文《比特币：一种点对点式的电子现金系统》说起。

比特币从09年正式出现，经历不到十年的时间，从技术宅的游戏跃然登上全球经济大舞台，其底层的区块链技术更被许多人认为是改革世界经济格局的一股重要力量。比特币到底是什么？

用最通俗的话解释，比特币就是一个不可被篡改的账本系统。这个账本系统的规则是事先定好的，通过共识机制保证其正常运转，无法改变。因此比特币通过其共识机制，保证了其总量的恒定，获得了和黄金、钻石一样的稀缺性。与争相被超发的

各国货币相比，比特币永远不会“通胀”。与大众甚至部分技术派的看法不同，毒蛇博士认为比特币的本质不是货币，也不可能成为流通的一般等价物，反而更接近于大宗商品，也就是黄金、白银等贵金属。

由于其数字货币的先驱地位，比特币成为数字货币世界的基石和基础交换媒介，一哥的江湖地位不可动摇，但是其对世界的最重要的贡献还不在于此。比特币的底层的区块链技术，以及其衍生出来的各种区块链项目和思想，才是比特币精神的真正延续。区块链技术通过竞争的观念创造出了基于代码的不信任的信任。在区块链的世界里，不存在信任的问题，因为节点和节点之间既互相猜疑，又相互信任。通过博弈论精彩的应用，机制精巧的设计，激励恰到好处的放置，区块链世界中的个体从不说谎，永远诚实，服从系统既定的规则，因为他们明白这是唯一最有利于他的选择。

总结一下，比特币的核心是账本，而区块链的核心是信任。

以太坊是基于区块链技术的第二代区块链项目，其思想是信任的自然延续，既然区块链能实现不信任的信任，为什么不用来创造可被信任的app呢？传统的app都是通过法律的监管和信用的约束来取得信任的，比如说微信钱包和支付宝，如果没有马云的信用，没有国家机器的监管，谁也不敢把钱存进去，万一马云明天跑路了怎么办？以太坊搭建了一个便于程序员开发的平台，使得可被信任的去中心化的app的开发变得非常简单。

无论是比特币、以太坊还是各种去中心化的app，都必须依赖“代币”，比如说比特币本质上就是一种代币，代币或者用来实现其基础功能，或者用于激励参与者依照事先约定好的机制行事。代币因此也身居三职，既有用户用于享受服务的功能，也有系统用于奖励的货币功能，同时具有区块链项目的股权性质。

因为一般来说，代币的使用量越大，也就是说需求越大，其价格越高。同时，如果投资者对某个项目的前景更加乐观，即使没有使用代币享受服务的需求，也会购买代币用于投资。因此，区块链项目的代币具有区块链项目的股权性质。与传统创业项目不同，区块链项目常常在非常初期向大众进行众筹募资，而不是接受天使投资人、VC的投资。这种募资被称为ICO，也就是initialcoinoffering，通过出售代币，也就是未来的服务和股权，换取大众的投资。

如此一番解释，大家有没有对数字货币的基本概念有跟深入的了解了呢？

区块链是泡沫吗？

感谢悟空问答邀请！欢迎点击右上角关注【令牌屋】，我们提供好玩有趣的区块链

电台栏目！

“比特币是泡沫吗”这个问题我经常看见有人问，但“区块链是泡沫吗”这个问题倒是第一次遇到。

楼主如果经历过2000年“互联网泡沫”就应该知道这种问题和当年是何其相似。98、99年是互联网喷发的时代，但紧接着互联网就遇到了“寒冬”，包括当年的网易、搜狐、新浪、雅虎等等都不好过，当时大家都在说互联网是泡沫。结果大浪淘沙，各大门户凭着彩铃业务死扛，最终活过来了，成就了现在的互联网。

那么，同样作为一项新兴技术——区块链是泡沫吗？还请楼主自己思考吧。

关于区块链，区块链与博弈论的介绍到此结束，希望对大家有所帮助。