大家好，关于比特币前世今生很多朋友都还不太明白，不过没关系，因为今天小编就来为大家分享关于比特币前世的今生的知识点，相信应该可以解决大家的一些困惑和问题，如果碰巧可以解决您的问题，还望关注下本站哦，希望对各位有所帮助！

本文目录

如何简明扼要、深入浅出的解释一下比特币和区块链？

这是一个很长的解释，我尽量的通俗易懂的解释一下。确实如果不去了解这个概念，是很难理解这个东西，并且认为是骗局之类的。

比特币与区块链的概念，诞生于2009年中本聪发布的论文《比特币：一种点对点的电子现金系统》。

先说区块链吧，几个比较重要的方面。

1.分布式账本，这个词出现的频率很高，那么这个分布式账本的具体含义是什么呢？就得从账本说起。最早的远古时期，人们打猎为生，获取了很多猎物，获得多少，吃了多少都是自己靠脑子记忆，随着人数越来越多，获得的猎物也越来越多，分配也越来越复杂，靠脑子就记不住了，于是就诞生了刻画与绘图，也就是最早期的记账。

随着时间推移，刻画与绘图也跟不上记账的需求，就诞生了结绳计数法。到这个时候可以称为是账本的起源了。

时间线继续推移，到达文明时期，社会发展空前繁荣，已经有了农业，畜牧业，手工业的诞生，文字也出现了，人们开始使用书契等文字叙述的方式来记账，按照收支事项发生的时间顺序来记录，也就是俗话说的记流水账。

随着文明的不断进步，流水账中也出现了日记账，现金出纳账的变种，也就是按时间，人名物品名，资金等分别设置的类似于账户的账本。这个时期的记账已经发展到了单式记账法时期。

从这个时期一直发展到近现代，记账法不停的发展，越来越复杂，比如中国的龙门账，四脚账等等，包括同期一系列西方的记账法，统称为复式记账法。

到了19世纪，信息技术爆炸式发展，企业的所有者和经营者都不再是一个人，更多的是一个集体，比如董事会，股东，公会等等，参与者都有着对账本的需求。而且需要处理的工作越来越复杂，逐渐的企业所有者与企业经营者的矛盾也诞生了，通俗的说，就是老板开始怀疑下面的员工做假账，源于这样的信任危机，就诞生了会计这个职业。之后，计算机技术的爆发式发展使得会计行业走向了新时代，即会计电算化。

前面说了这么多，总算要说到分布式账本了。到了现在的时间点，虽然记账手段层出不穷，但是有个最根本上的问题，就是存在信息不对称以及信用问题。

举个例子，如果没有得到完全正确并且公开的信息时，你如何信任一个会计或者审计给你做的项目？会不会怀疑会计勾结公司做假账呢？区块链就是给了这样的一个解决方案，分布式账本。

这个账本有三个特点。

1.可以无限增加的巨型账本，每一个区块可以当做这个账本的一页。

2.加密且有序的账本，项目信息会被打包成为一个区块并且基于密码学技术来加密，同事盖上时间戳，一个个区块按照时间戳顺序连接起来形成一个总账本。

3.去中心化的账本，以往的账本都是由某个人或者某个机构又或者某个服务器来运行维护，也只有那一个中心拥有。而去中心化也是由网络内用户共同拥有并且维护，所以是去中心化的。

这就是区块链是一个分布式账本的解释。虽然很长。

2.价值转移。自从互联网诞生之后，我们的生活进入了一个信息爆炸的时代。各种信息传输技术遍地开花，断点续传，点对点，云盘等等。但是渐渐的，会发现很多信息只需要简单的复制粘贴就可以使用，比如文字，视频，图片等等。但是有些信息却是无法复制的，复制也没有意义。

最简单的，我们不能直接把钱在网络上复制给对方，而是要在付款账户减去金额，在收款账户加上金额，才能完成支付过程。一个图片可以复制到另一个网站上，那么两个网站都可以看到这个图片，大家都可以分享。但是对于支付行为来说，是只能转移而不能分享，而这类需要转移的有价值的信息往往需要信用背书。互联网解

决了信息分享呢问题，但是不能解决价值转移的问题。

再详细一点描述价值转移吧。比如我要在互联网上转账100块钱给某个人，那么需要将我的账户精确的减少这100元，并且对方的账户要精确的增加这100元。这个价值转移设计到我和对方两个独立的参与者，那么这个操作就必须使得我和对方都认可，并且这个操作结果还不能收到双方任意一方的操纵。目前的互联网协议是不支持价值转移的，他无法判断你的数据信息是否有价值，所以目前互联网上的价值转移都是由一个中心化的第三方来做信任背书，比如支付宝，微信。

现如今中心化机构通过政府或者集团公司来完成背书，把所有价值转移的计算放在一个中心化的服务器中处理，其中一定会涉及到人的参与，而人的“机会主义理论”往往会使得整个系统变得不那么信任。这时候又一个最基本的问题出来了，如何达成信用共识？

于是区块链技术就这样诞生了。它可以在没有第三方信用背书的情况下，在一个开放式的平台进行远距离的安全的价值转移。所以不依靠第三方的信用背书才是区块链的特点。

区块链网络中所有授权的参与者都保存着一份完全相同的账本，一旦对账本进行修改，全部副本的数据必须在同时全部修改完毕，这就是分布式账本的优势。

可以说，区块链可以构建了一种纯粹的点对点的价值转移体系，在不需要各节点相互信任的情况下，区块链可以保证系统内数据记录的完整性与安全性，可以脱离第三方机构背书，有效的降低交易的复杂性和风险。

写的太长了。由于区块链概念确实很难理解，我就暂时写到这里，较为详细的介绍了其中比较重要的两点。

关于比特币的话，等我有时间再码字吧，内容太多了。

如果你觉得我的答案不错，欢迎点赞关注，也可以相互交流。

比特币的发明人中本聪是谁？

2018年10月31日，中本聪在密码学邮件组发表了题为《比特币：点对点的电子现金系统》的论文，阐述了一种新的电子现金系统，用户可以直接交易，无需任何可信的第三方。

2009年1月3日，比特币区块链的第一个区块（称为创世区块）诞生，由中本聪创

造。一周后，中本聪发送了十个比特币给密码学家哈尔·芬尼，这成为了比特币历史上的第一次交易。

中本聪，作为比特币的开发者兼创始者，一直是个迷。中本聪是化名，至今无人知晓这是独行侠还是团伙？还有，为什么要取日文名字？是因为东方神秘主义？与悬念侦探小说有关？很多疑问至今仍然无解。

比特币2008年问世，中本聪2011年在网上抛出若干有关比特币的白皮书，随后神秘消失。之后，各方人士搜寻了10多年，仍无法查出其真实身份，甚至完全断了线索。2016年，一个名叫雷格·赖特的澳大利亚人冒了出来，非说自己是中本聪，但很快被认定为冒牌货。也有人主张，没必要满世界找中本聪。有个名叫安德烈亚斯·安东诺波罗马斯的比特币业务企业家说：“比特币是信任的中性框架，数十亿人可借此在金融方面自力更生。之所以能够做到这点，是因为不需要任何人的权威，甚至不需要中本聪的权威。

中本聪的真实身份无从知晓，其言论也可能是他人盗用其名在网上发表的。中本聪何以不愿暴露真实身份？首先，中本聪有很大的利益冲突。据称，到2015年，中本聪所持有的比特币已价值4.48亿美元。按中本聪的设计，总共只能设计2100万个比特币，预计2140年将全部售完，他是否还有其他伏笔仍是悬念。可见，中本聪深藏不露并非出于公心，他有巨大的经济利益。不愿出面回答各种问题，还有个原因：为了个人安全，害怕现代“梁山好汉”上演现代版“智取生辰纲”。

不过，比特币也有种种问题。比如，比特币的价格飞速飙升，其泡沫远大于银行信贷的泡沫。即便中本聪菩萨心肠，事事出于公心，许多问题还是他始料不及的，网上交易比特币费时费电便是一例。还有，比特币为不法分子从事犯罪活动提供了便利。

找不到中本聪，比特币很多问题便无法求证。不过，即便中本聪现身，愿意老实交代，很多问题也是他根本没料到的，也就无从交代。

比特币为什么这么稀有？

1、比特币起源

想完全了解比特币的起源，不得不提现有的金融体系。

众所周知，货币本身是不存在价值的。起初人类采用以物易物的方式进行交易，但有诸多不便，很难换到自己所需要的物品。于是货币应运而生，通过货币这一中介，可以将不同物品按稀有程度进行定价，简化交易流程。

虽然货币交易好处多多，但也有一个致命的缺点，那就是中心化。全世界现有货币100%是国家央行发行或者废除，普通人无法参与货币发行亦或者是央行帐目。如果央行不断的发行货币，将会将人们手中的货币不断稀释，降低货币购买力。

这绝不是危言耸听，世界上一些国家已经发生过此类事件。

比如津巴布韦，近年来政府大量超发货币导致津巴布韦经济接近崩溃，最后不得不将美元引入成为当地法定货币。现在津巴布韦经济学家们正在考虑比特币替代方案。

比如印度，印度官方在2016年11月8日突然宣布，面额为500卢比(价值7美元)和1000卢比(价值15美元)的钞票9号凌晨废除，此举导致印度民众手中的85%财产瞬间变为废纸。

为了解决此问题，比特币之父中本聪于2009年提出去中心化概念，也就是说将货币发行在开源软件以及建构其上的P2P网络，打造一个去中心化的支付系统。很多读者看到这又不明白了，什么是去中心化?什么是P2P网络?

我们以国内流行的微信支付举例，微信虽然和比特币同为虚拟支付系统，但微信的每一笔交易都要在银行系统中进行，银行便是微信支付的中心。去中心化即是点对点交易，不受任何其他因素影响。

P2P网络更好理解，P2P是peer-to-peer的缩写，就是“伙伴对伙伴”，也称之为对等网络。比如你通过爱奇艺下载一个电影，就是从爱奇艺服务器将电影传输至你的电脑;而如果你从P2P资源下载一个电影，便是从其他已有此电影资源的P2P用户电脑中下载，并且如果其他P2P用户需要此资源，也可以从你的电脑里下载。

比特币就像这部电影，它不是像央行一样存在中央服务器中，而是存在于世界上亿万的电脑之中。自发行后，理论上没有任何人可以控制比特币数量，也无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付，安全性极佳。

不过比特币并不完美，有一个致命缺陷导致它无法成为法定货币，这点我们下文会讲到。

2、比特币是怎么产出的?

首先我们来了解一下“区块链”，比特币的核心原理是“区块链”，每一个区块对应一个帐单，将所有的区块链接起来就是区块链，任何交易信息和转账记录都记录

在区块链中。要注意的是区块链存在于整个互联网中，所以任何比特币持有者都不担心比特币遭受损失。

每隔一个时间点，比特币系统会在系统节点上生成一个随机代码，互联网中的所有计算机都可以去寻找此代码，谁找到此代码，就会产生一个区块，随即得到一个比特币，这个过程就是人们常说的挖矿。计算这个随机代码需要大量的GPU运算，于是矿工们采购海量显卡用以更快速的获得比特币获利，这也是近期显卡缺货的重要原因。

有人说那这样比特币不就会越来越多，最后完全没有价值了吗?中本聪当然也想到这个问题，这里比特币系统还有一个机制：那就是比特币具有总量有限，前4年总额将产生10500000BTC，每隔4年产出数额减半，在第4年至第8年会产生5250000BTC，第8至12年则只有2625000BTC，如此类推。到最后，总共产生的比特币数量为接近21000000BTC。

目前一个1个比特币基于目前的数据结构被分割到8个小数位，也就是0.00000001BTC，矿工们挖到比特币最小的单位就是0.00000001BTC。

通俗点说，比特币好比是一座由总量为2100万个金币组成的金山，想要得到它，就需要玩家们利用电脑的运算能力，根据现有的算法计算出一组符合特定规律的数字。

当然，这些数学题随着现有比特币的增加正变得越来越难。

3、比特币为何能产生价值?有何弊端?

其实这个问题本身就是错误的，上文也曾提到，任何货币本身是不存在价值的，只有足够数量的人相信货币，才会使货币产生“价值”，并且这个”价值”是带有引号的。但现在很多人相信比特币可以为他们带来财富，所以比特币才产生了“价值”。

让我们来回顾一下比特币的特点。

1、总量有限，只有21000000BTC

2、任何人都可以发行比特币，但发行难度越来越大

3、相对央行货币更安全，几乎无法被盗

4、交易过程完全匿名，不能追踪

基于以上优势，越来越多的人开始愿意将他们的财富转换成等值比特币，同时取消这些财富的法币代表权，所以比特币价格才开始不断的上涨。相信比特币的人越多，比特币价格涨势便会越凶猛。当然，前几日比特币暴涨21000元又跌落至17000元事件属于投机炒作行为，比特币长期的优势是不能被投机所左右的，最终比特币一定会相对稳定在它所真正代表的财富总值上，但现阶段，比特币的价格波动还是太剧烈了。

从现阶段比特币的表现来看，比特币流动性水平较低、流动性风险较高，因此无法有效履行货币的交易媒介、计价单位以及价值储藏三项基本职能，无法成为真正的货币。

再加上比特币总数量有限，通缩现象会变得越来越严重。试想若用比特币取代全球货币，如果一人拥有10，500，000BTC，今后的岁月里，他将拥有世界上一半的财产!并且要注意这份财富是永久的。所以比特币想完全取代货币，是完全不可能的。

4、挖矿收益分析

最后我们来谈谈挖矿收益分析，挖矿成本主要包换：矿机(也可以是普通家用电脑)、电费、房屋租金。由于比特币算力太过复杂，ZOL评测室的电脑工作数月也可能毫无进展，所以这里我们以——以太币(一种类似比特币的虚拟货币)挖矿为例，为大家进行了主流显卡挖矿收益实验。

对于挖矿来说，显卡是核心，其余都是辅助配件，考虑到每个人使用平台各不相同，这里考量的挖矿成本就只包含显卡价格、电费，电费我们参考北京的阶梯电价第二档0.5383元/千瓦时。

具体测试成绩如下：

【RadeonRX580显卡】

整机功耗：243W

计算力：22.4M

显卡售价：1999元

每24小时挖ETH数量：0.015

每24小时产生收益：24.48元

预计回本时间：81.66天

【RadeonRX470显卡】

整机功耗：159W

计算力：24.3M

显卡售价：1599元

每24小时挖ETH数量：0.017

每24小时产生收益：27.9元

预计回本时间：57.31天

【RadeonRX480显卡】

整机功耗：171W

计算力：24.4M

显卡售价：1999元

每24小时挖ETH数量：0.017

每24小时产生收益：27.87元

预计回本时间：71.73天

【RadeonRX560显卡】

整机功耗：97W

计算力：9.2

显卡售价：999元

每24小时挖ETH数量：0.006

每24小时产生收益：10.09元

预计回本时间：99.01天

【GeForceGTX1060显卡】

整机功耗：175W

计算力：22M

显卡售价：1999元

每24小时挖ETH数量：0.015

每24小时产生收益：24.86元

预计回本时间：80.41天

【GeForceGTX1070显卡】

整机功耗：220W

计算力：25.7M

显卡售价：2899元

每24小时挖ETH数量：0.017

每24小时产生收益：28.84元

预计回本时间：100.52天

综上数据可以发现，RadeonRX470显卡回本速度最快，仅需57.31天。而GeForceGTX1070整体效率最差，需要100.52天才能回本。

不过各位读者请注意，本次测试回本时间仅以显卡价值计算，并未计算平台成本以及场地成本。挖矿机实际运行中突然情况非常多，比如宕机、硬件损坏，停电等等。所以打算挖矿的读者们还请慎重考虑，若非有极低成本电力，挖矿很难盈利。

写在最后：

随着无现金社会的有序推行，纸币必然将随着时间的流逝消失在历史的长河中。而未来的数字货币相信会和比特币类似，但绝不是有限供给。

而是当人类的生产财富的能力完全可以由计算机的计算能力匹配的时候，电子货币的发行速度和计算机计算速度成正比或者略微超出一定比率以制造温和通胀，在未来挖矿的同时也是在创造价值而不是现在的浪费电力。

最终数字货币实现生产力的微小变动和计算能力难度所匹配，这或许就是人类货币的最终形态吧!

比特币已经一币一轿车了，距离一币一别墅还会远吗？

接下去应该是区块链爆发的几年，越来越多应用会使用这技术，只要开发团队跟上步伐，个人认为前景还是广阔的。当然他的上下波动会很大，想要加入一定要利用闲余资金投资（绝对不要贷款倾其所有投入，很容易导致心境不稳，90%会亏），属于高风险高回报类型。一定要静心，耐心等待！

虽然比特币属于这方面鼻祖，但是个人认为可以多方面（个人对bch认可更高）选择，但是他还是相对其他币种而已比较稳的。

比特币前世今生和比特币前世的今生的问题分享结束啦，以上的文章解决了您的问题吗？欢迎您下次再来哦！