

大家好，关于比特币第四轮价格周期很多朋友都还不太明白，今天小编就来为大家分享关于比特币第四轮价格周期走势的知识，希望对各位有所帮助！

本文目录

- [1. 七年涨了360万倍，比特币会成为世界第四大金融泡沫吗？](#)
- [2. 比特币挖矿到底在计算什么？](#)
- [3. 币圈九四是什么意思](#)
- [4. 比特币18年会继续下跌吗？](#)

七年涨了360万倍，比特币会成为世界第四大金融泡沫吗？

比特币暴涨跟其自身机制有关。

现代信用货币受货币国家货币当局的调控，自身价值不会剧烈波动，因而不会被恶意炒作。数字货币不是任何国家和地区的法定货币，也没有政府当局为它提供担保，没有集中发行方，容易陷入过度炒作，导致价格过山车。币值的剧烈波动又提供了巨大套利空间，进一步推动过度炒作，形成恶性循环。比华尔街疯狂百倍的数字货币市场，全球7x24小时无休止交易，动辄百倍千倍的上涨，大量进场毫无计算机基础只追求利润的赌徒，终于招致全球监管的出离愤怒。

其实桃李不言，下自成蹊。比特币作为一种利益激励机制很好的发挥了财富效应的作用。任何一个新应产业的发展都需要财富效应的推动，尽管有可能会存在泡沫，但是泡沫确实一定程度上，推动着新技术的快速进化。

比特币挖矿到底在计算什么？

BTC的价值就是交易渠道本身。一组新制造出来的比特币提供了把旧的比特币从一个帐户转移到另一个帐户的数学保证。这个安全保证背后的代价是大量的计算力。生产这么一个安全通道是需要消耗大量能源的，所以整个比特币用户群体，奖励那个造币者（目前是50BTC）。

简单说，我的理解就是，现在世界上所有的比特币背后都是用运行计算机的能量产生出来的，它们的总价值，（到现在一共有大约12w组比特币被生产出来，每组50个，市场价格大约7.3美金一个），应该是少于消耗掉的能源的总市场价值的。不过我想，用于生产比特币的能源大都原本就是不用也被浪费掉的资源。

一个没有中心节点的“银行”是怎么让大家信任并工作起来的呢？

答案是，这个p2p网络上每个节点都记录了比特币诞生以来的每笔交易的详单，并从中可以推测出每个比特币唯一的属于谁。这样你接受一笔交易时，就能知道别人给你的钱是不是合法的。

从最基本的说起：

每个帐户其实就是一对公私匙，有私匙的人就是帐户的主人。如果A要给B转一笔钱，A就把钱的数量加上B的公匙，用自己的钥匙签名。而B看到这个签名，就可以了解，的确是A转给了他如数的比特币。

那么这笔交易需要一个见证人，担保交易发生过。这样，以后B想用这笔钱的时候才是合法的。担保人就是整个使用比特币的网络。

A在发起这笔交易的时候，必须把签过名的交易单尽可能的广播到p2p网络上，最终会让每个节点都知道这件事。B从p2p网络上不断的收到别人的确认信息。当它收到足够多的确认信息后，就认为A的确发出了这条交易单。这以后，B就可以自由使用这笔钱了。

当B使用A转给它的钱给C时，也会广播给足够多（最终所有人都收到）的人让他们担保。每个担保人只有确信B有足够多的钱可以支付的时候才做确认。本质上，BTC网络并没有记录每一块钱属于谁，它记录的是从诞生起到当前的每一笔交易，并推算出每个帐户里有多少钱。任何人试图确认一个交易单时，它需要确认的是转出帐号上有没有那么多钱。

比特币需要解决的核心问题是，如何避免一笔钱被花两次。

整个帐单序列是一环套一环的。每个人在完整的全局帐单上签上新的一笔的时候，都需要利用前面信息生成后面的。这个帐单序列被称为chainofblocks。每个区块里面包含有若干条经过确认并hash签名（难以伪造）的交易记录。每个区块都和全局表上的上一个区块有关联。每条帐单都会通过p2p网络最终被转发给制造新区块的节点上。

这个制造新区块的过程被叫做挖矿，制造新区块就是把最近收到的帐单打包在刚制造的区块里。这个打包的过程即制作的过程，只有极其稀少的几率被制造成功。（你可以理解成把新收到的帐单合在一起，一次成型不可修改，如果制造失败就要再来一次）一旦制造成功，你就把新的区块（被认为是对老的全局区块链的延续）广播出去。

因为是p2p网络，可能有许多人都在同时制造新的区块，但有一个排序机制保证只

有最优（最难，花费最大计算时间的）的那个新区块被网络群体接受，挂在全局的区块链上。重复一次，整个比特币网络只有一个全局帐单表，每个节点都完整的保存有一份。

这个全局帐单表会越来越大，区块链越来越长，在最新的部分，必然有许多分枝。这是因为p2p网络的挖矿过程是分开并行进行的，每条新帐单也不能立刻广播给所有的节点。每个挖矿的节点都有责任把他新收到的，在他认可的的老的全局帐单上不存在的帐单，合在他准备制造的新区块中。一旦新区块被制造出来，就立刻广播出去，争取得到更多人的认可。主要是得到那些想挖矿的人的认可，这些人会在这个区块的基础上制造新的区块。

如果p2p网络过大，交易帐单不能尽量的迅速的广播到全网络。就会出来p2p的网络的局部保持有小群体共同认可的一份全局帐单。多个全局帐单的分支同时发展是有可能的。因为每个小群体都可能认为他们看见的那部分更长更有效。但是，只有有人发现另一条分支更长，它就会转换阵营。所以，有一定的可能性，你的帐单被一个小群体接受，但在一段时间后，被更大的阵营抛弃。

不过，算法参数决定了，新的区块产生速度很慢，如果你的帐单被多达6个人确认，基本上就保证了它合并到的那份全局帐单，就是p2p网络全体认可的。

既然生成新区块费时费力，制造出新区块的几率好象买彩票中大奖，还有那么多人去执行程序计算出新区块呢？答案是，每个制造出新区块的人，都有权利构造一条帐单声明老天给了我50比特币。这个规则是被所有比特币用户共同承认的。把制造区块等同于成挖金矿(mining)只是一个形象上的比喻。实际上，没有人可以把金子挖出来囤积。每个新区块必须包含全局表上的上一个区块的hash值，BTC网络自我调节难度，让每10分钟大约产生一个新区块。如果你10分钟内没制造出新的区块，差不多就是说你前面10分钟干的活白干了。从最新版的区块继续演算。

所以更恰当的比喻是买彩票。一个每10分钟开一次的彩票。你不停的花钱买，10分钟内开中了就是你的，开不中先买的都作废，然后下一轮。

数学上怎样保证挖矿的过程需要消耗大量的CPU时间？并只有很小的几率成功？

这里用到一个叫做Hashcash的系统。它最早是为了改善emailspam的问题被发明出来的。

就是给一段特定信息（比如这封email是从谁发给谁）加一个特定的hash头。这个hash头需要大量的CPU时间计算出来。发spam的人没有那么多CPU时间为群发的每一封email计算一个符合要求的hash头，所以认为有这个合法hash头的email不

太可能是spam (花了CPU时间在上面)

这个算法就是，为你想保护的信息，找到一串数字，附加上去后，使用某种公认的hash算法，比如SHA-2，算出一个hash值。如果hash值由一长串0打头（具体多少个决定了难度），那么就成功了。

为一段信息，找到这串数字，在目前来说，除了暴力尝试没有什么好的方法。也就是随机更换数字，换一次就hash一次比对。在一个可以预期的尝试次数后，一般都能找到想找的数字。

每个想挖矿赚比特币的人，不停的从比特币网络上监听信息。如果有人发布了新的合法的区块，他就合并到本地的全局表里。并重置自己的计算过程，从新得到的区块开始。如果有新发布的交易单，也记录下来。不断的把最新的区块的hash值、新收到的交易单，自己获得50比特币的那条奖励单合并在一起，计算SHA-256，看看结果是否满足条件。一旦满足，就把这个新的区块广播出去。

当足够的人认可它，（以它为基础计算后面的区块），他也就获得了那50比特币。

为了匹配比特币的经济规模。所有的比特币client都被设置成，每210000个区块，生产新区块的人被认可凭空获得的比特币数量比之前的少一半（如果这个时候他还在包内写上自己获得50比特币，其他人不会确认他的这个区块）。这会让比特币的总量增速变缓。新的区块产生的速度是由难度来调节的。这个难度会由p2p网络根据最近生产区块的速度自动调节。所以即使日后计算能力增加，也能保证大约10分钟一个的速度。

而且，随着生产新区块的收益减少，愿意贡献自己的CPU来挖矿的节点也会变少。（如果减少太多，只需要减少难度即可）

最终，p2p网络不再凭空制造出新的比特币，这个时候制造新的区块的动力是什么呢？那就是交易税。因为没有什么人愿意生产新的区块，发起交易就变的困难。（没有区块可以容纳交易单）希望交易被确认的人可以声明，如果有人制造出新的区块接纳他的交易单，他会支付一小笔交易税给他。当许多人都这么做的时候，制造区块又变的有利可图了。只不过，直接上不再有新的比特币诞生，只是在这些比特币用户之间流通。

总有一些比特币会消失，主要是那些帐号的私匙丢失了，没有任何人可以转移走帐户上的钱。不能流通的货币就不是货币了。但最终比特币总体会达到一个比较大的规模，准确说是两千一百万个。但比特币本身是可以切割的，比如你可以支付给别

人0.01个比特币。所以比特币本身会升值，总数也一直够用。

币圈九四是什么意思

回答:币圈九四，是指2018年4月9日比特币价格下跌至最低点。这一天被称为“九四”，因为数字9和4谐音“鸟蛋”在币圈中被用作“暴跌”的代称。在那一天，比特币价格跌破6500美元，并且许多加密货币市场也出现了巨大的跌幅，许多投资者遭遇了重大损失。

比特币18年会继续下跌吗？

可能会有调整性下跌，但是总体看涨

比特币是虚拟货币的代表。从其一面世，就是一路血雨腥风。从2012到2016年前经历了价格低谷。从2016年以后又开始一路变态的猛涨，最高价格超过20000美金一枚。当然到2018年后价格有所回落。

我想看比特币是价格的涨跌，应该从几个方面来分析！俗话说：内行看门道，外行看热闹，以下分析仅代表我这个外行人的意见。当然我也曾经持有过一段比特币。数量不多4个，当时以大概5000左右人民币入手。可惜在2016年比特币期货市场最火爆的时候抛出，然后资金全部仍在了期货市场，惨败而归。当然看到今年最高每一枚高达20000美金，的确有点懊恼。不过资本市场就这样，神仙都不一定会踩准点，更别提我等凡夫俗子。

1、市场需求

2017年以来，资本市场炒的最火热的肯定就是区块链概念。区块链简单的说，就是一种去中心化的信息加密储存方式，最大的特点就是不可篡改。具体的大家想了解就去百度一下。或者就在头条上搜索一下，其中也有很多大V讲的非常详细。比特币就是区块链概念的一个典型产物，虚拟货币。由于其数量是有限的，全世界2100万颗，其次就是伴随着区块链技术的运用，比特币甚至很有可能成为世界流通币种使用。所以在这一概念上，大家明白，如果需要做一些资产配置或者转移什么的。这个肯定是组好的方法。不知道说了会不会被XX。比如前几天上海举办的区块链论坛，就有运用区块链技术研究的取款机，可以直接用比特币兑换取出任何币种。

2、入市场景

在2017年上半年基本还可以做比特币期货甚至在2016年还可以做杠杆。当然我个

人也是因为在比特币期货市场玩杠杆最后全军覆没。后来随着政策的调整，现实不能进行杠杆操作，后来就逐渐在国内关闭了所有期货交易市场。只能进行C2C的实物交易。这样相对比特币高额的单价来说，缺少了期货市场和杠杆资本，对于爱投机的国人来说，可能逐渐就会失去兴趣。

3、多虚拟币币种的出现

随着区块链概念的日趋成熟。区块链技术逐渐运用。很多虚拟币也开始出现。投资者们选择空间就会更大，会逐渐把眼光放到一些起步价格不高，但是又有长期持有价值的币种。而且在虚拟币市场除了比特币，也有通过其他币种，比如以太币等等，一夜暴富的。

4、长期持有会逐渐增多

目前比特币因为数量有限，加之是属于区块链的概念去中心的情况。所以，大部分币还是持有在少数的人手中。不是前段时间都曝出中国首富李嘉诚手中也持有大量的比特币。而这类人基本将比特币当做资本储备，会长期持有，完全不会急着出手用来作为投资。所以市面上的比重就会越来越少。

所以，基于我以上4点看法，觉得比特币如果会在短时间类疯狂上涨应该不太现实。但是长期肯定是很具有大的上涨空间。如果需要做投资的话，适合长期持有。不适合短期投资，当然如果很多人愿意搬砖的话，也没什么关系。

比特币第四轮价格周期和比特币第四轮价格周期走势的问题分享结束啦，以上的文章解决了您的问题吗？欢迎您下次再来哦！