大家好，今天来为大家解答比特币小额这个问题的一些问题点，包括比特币大额也一样很多人还不知道，因此呢，今天就来为大家分析分析，现在让我们一起来看看吧！如果解决了您的问题，还望您关注下本站哦，谢谢~

本文目录

1. 请问比特币区块链中，比特币，口碑怎么样？
2. 如果靠卖比特币赚了十亿，那这笔钱我可以顺利提现到个人账户吗？
3. 比特币是否是一个大骗局？有人玩比特币吗？
4. Bitcoin（比特币）的技术设计是否支持大规模应用？

请问比特币区块链中，比特币，口碑怎么样？

比特币是一个账本

比特币让人们的电子支付和发一封邮件一样简单。给别人转账的时候，你要用到手机上的钱包软件，输入金额，扫描一下对方的账号，点击发送。这样对方就看到自己账号上有了新的进账了。

那这一切是怎么工作的呢？最基本的，比特币就是一个账本，上面有账号和账户余额。当Bob给Jim5个币，那他的账号余额就减少5，Jim的加5。比特币背后没有政府和黄金的支撑，它纯粹基于人们对它的购买力的认可。系统可以提供安全保障，没有人可以随便修改账本。

没有人可以随便花别人的钱。每次你点击发送，钱包软件就会向比特币网络发送一条信息，告诉账本应该怎样变化，信息包含数额，发款和收款人账户。但是如何防止有贼挪用他人账号上的钱呢？每条信息都配有一条签名，来保障信息是由账号的主人发出的。这和支票上的签名是类似的。只不过这里的签名是数学方法生成的，而不是手写的。数学方法来自加密学，通常是用来给机密的信息做加密解密用的，但是用在比特币这里主要是为了确认身份。

每一个比特币账号都有一个秘钥，只有账号主人才知道。它可以用来加密信息，来生成签名。这样，他人就可以通过解密签名来验证签署人身份。如果验证成功，就可以证明信息是真的从账号主人那里发出的。数字签名还有个好处，就是不能拷贝复用，因为每次交易的签名都不同。

有了签名，那么伪造的信息就不能更改账本了。但是，是谁来验证签名，维护账本的呢？可能会让你感到惊讶的是，任何人都可以。比特币系统的一个大的设计目标是，制造一个分布的去中心的系统，不被某个政府或公司控制。每次有人付款，交

易信息就会传递给网路上的所有账本维护者。每个维护者，都有账本的一个拷贝，收到信息后就会更新自己的拷贝，只要签名验证是通过的。

通过数学赛跑来投票

但是网路上经常会有延迟，也会收到恶意伪造，所有所有的这些账本拷贝，同一时刻很难达到一致。那么大家到底要相信谁的那个账本呢？和其他的民主系统一样，通过投票决定。投票的方式是大家都运算一个跟自己这个账本数据相关的一个数学结果。第一个算出答案来的人，就广播出答案和他自己的账本信息，其他人的账本就根据他的账本做更新。投票实际上就是一种数学上的赛跑，让最大多数人的那个账本很容易胜出。因为越多的人运算一个相同的版本，那这个版本就最有可能胜出。系统上的交易会不断生成，那这个赛跑也会周而复始的进行，让大家不断保持账本统一。

那为啥采用数学方式？而不是让大家发邮件来投票？因为没有统一管理，所以如果有坏人自己伪装成很多人，也就无法辨别。比特币系统的解决方案就是让你每次投票都有真金白银的成本，因为参加数学赛跑需要买计算机和花电费。这也就意味着如果坏人想在投票中取胜，那他就得比所有诚实的人花钱的总和还有多。总之，数学方法实现了在去中心化的系统中公平投票的一种机制。

相关的两个细节。第一，为了防止有人提前运算，每次运算都基于前面一次运算的结果。第二，运算过程是没有窍门的，想要算的快只能去多买强大的计算机。这样，最终可以保证结果是来自最大多数人的，而不是聪明的攻击者。

钱的发行

最后说说，比特币的发行。每次有账本维护人算出结果，系统就会给他一定数额的比特币作为奖励，这样维护账本的人就有动力了。另外发款人也会付一个小额的手续费。因为维护人挖到了币，所以通常人们把他们叫矿工，但是矿工最重要的目的不是挖钱，而是维护账本。整个投票系统可以让比特币随机的被发行到世界的任何地方，到2140年就不会有新的比特币被挖出来了。

总结。比特币是一个基于大众协作维护的账本的电子货币。发款的时候，就给维护人发一条信息，说明钱要转到哪里，数额是多少。维护人负责检查数字签名，保证信息是账号所有人发出的。各个维护人之间通过投票的方式达成一致。

如果靠卖比特币赚了十亿，那这笔钱我可以顺利提现到个人账户吗？

交易所卖掉换usdt、usdc、pax稳定币倒是简单，挂币安估计一两个小时肯定卖掉

了，难点在于USDT等换成人民币，主要是套现这么多，一定会触发银行风控，然后就会打麻烦，一旦银行为了保险起见严格执行五部委文件，你就得把钱提走换个银行，就算这样可以，一次500万500万卖，也要卖好久。

而且卖的时候币价还会跌。

另外一种方法是场外交易，专业的场外交易团队，千八百个比特币出掉是不难的，毕竟现在圈子也大了，同行都有联系，大单子吃不下大家分一分就行了。

但是资金汇聚到银行卡上，还是会触发银行风控，法律方面没风险，就是打麻烦，银行会追问你的资金来源，需要提供材料，然后还是有可能触发执行五部委文件精神。

要我说，你还是留着一半卖一半，卖出来的换成usdc（合规稳定币），需要钱的时候就场外交易卖点出来，隔几个月卖三五十万百八十万，那问题就不大了，至于美元贬值就贬值吧，怕贬值BTC就别卖，零利率总比负利率强。

比特币是否是一个大骗局？有人玩比特币吗？

这个问题问的很尖锐，有点不是太好回答。说不是骗局吧很多人觉得虚拟货币就是一个泡沫没有任何的实际应用价值，说比特币是骗局却又经历了四次完整的牛熊市依旧立而不倒，总的来讲我们要去辩证的去看待新事物的发展。

比特币的背后代表的是一种时代潮流。

很多人是通过比特币的暴涨才知道了区块链这种技术，九年时间1300万倍的涨幅吸引了太多投资者的目光。而比特币底层所应用的区块链技术则是一种新兴的技术，数字货币是区块链金融领域的成熟应用。

存在就有价值有需求才会有市场。

很多人并不清楚比特币这种毫无实际应用价值的代码到底有何使用价值？其实比特币的出现完美的契合了也不能见光的市场需求，比如暗网黑市走私等地下市场交易。点对点的交易模式和加密不可追踪性极大的促进了比特币的流通和认可。有阳光的背后就有黑暗这个世界确实是非黑即白有时也会存在灰色。

目前的比特币正处于牛熊转换之间，最近的世界杯影响整个市场不管是币市还是股市资金都出现了撤市，而比特币的价格甚至一度接近2月份暴跌的最低点。这是市场的自然洗盘也是去除一部分的市场泡沫，拥有一定得完善机制，如果不去除泡沫

后果很严重，而完全去除泡沫比特币市场将不复存在。

总得来讲：还坚持认为比特币是骗局的可以远离比特币，去关注他也不去了解他让他自生自灭。认为比特币值得投资的可以闲钱适度投资是仁者见仁智者见智，目前为止并没有出现唯一的答案。

Bitcoin（比特币）的技术设计是否支持大规模应用？

以比特币为代表的公有区块链系统一直有一个广为诟病的缺点：交易性能低。

交易性能低包括两方面内容：一是交易吞吐量小，二是交易速度慢。交易吞吐量是指系统在单位时间内处理请求的交易数量；交易速度是指系统对交易从提交请求到确认交易成功的平均时间。在比特币区块链系统中，这两个值低得可怜。交易吞吐量是平均每秒7笔，交易速度是平均1小时能完成交易确认。对比一下一般商业银行的核心系统交易处理能力，交易吞吐量一般都要超过每秒2000笔，交易速度一般要达到实时。

正是由于比特币区块链的交易性能太低了，所以很多人都认为这个性能缺陷导致了比特币无法成为一种用于交易的货币。是什么原因导致了比特币区块链系统的交易性能低呢？

区块链作为一种分布式账本技术，核心功能是要把账目都记下来。通常公有区块链的记账方式相当于每个人都在一页账页上一条一条的记录交易，记录了一定时间后，通过某种竞争办法选出记录的最好的一张纸，大家都复制一份，添到自己的账本上，然后开始新的账页记录和竞争。

这里面有两个限制：账页的大小和记账的周期。账页大小确定了每个区块所能容纳的交易数量，每个区块容纳的交易数量除以记账周期就是交易吞吐量；

而记账周期则直接决定了交易确认时间，记账周期乘以大概率确认区块有效性的区块数（比如比特币里我们通常认为6个区块基本上就能确定交易有效）就是交易确认时间。

要想提升公有区块链的性能，最直接的办法就是增加每个账页内的交易数量（区块扩容）和减少记账周期。（比特币的扩容之争，以及比特币现金（BitCoinCash）的出现，就是区块扩容引起的。以后我们会详细讲这个问题）对于区块扩容，通常直接影响到区块的传播速度。当然，以现在的网络带宽和速度来看，比特币当初确定的1MB大小的区块确实是比较小，但是小区块也有小区块的好处——可以采用更多的通讯方式进行传播，比如卫星通讯。减小记账周期，则会影响到区块传播的范

围。

如果区块过大并且记账周期太短，就会造成去中心化程度的降低。原因很简单，当一个矿工挖到了一个区块后，其他矿工还在下载接收这个区块的时候，他已经开始挖下一个区块了。显然，接收一个区块所占用的时间在一个记账周期中的比例越低，对于全体矿工来说就越公平。否则，先发优势过于明显，导致整个系统的去中心化程度降低。与此同时，整个网络同时挖出块的概率将会大大增加，就会需要更加复杂的机制来解决这个问题。

因此，对于公有链来说，用改变区块链自身的方式来提升区块链的交易性能，想要追赶现在金融系统的交易处理能力，难度还是非常高的。换句话说，我们想提高公有链的链内交易的交易性能，难度极大。

转回头看看传统金融系统的结构。在我国，不同的商业银行通过央行提供的大小额支付系统实现了跨行交易。而普通用户在使用银行系统的时候，很多交易都是在同一个银行内进行的，只有涉及到跨行交易的时候，交易数据才会被提交到央行的系统上进行处理。因此，大小额支付系统上的交易数大大降低了。

区块链上也可以采用类似的办法来解决。我们把这种方式统一叫做链外交易。也就是说，某一个组织或者机构可以提供一些服务，让我们在链外记录这些交易，每隔一定的时间，把这些交易的结果写入区块链即可。举例来说：Alice、Bob、Charlie、Dave4个人之间发生了一系列交易：一开始每个人都有100美元，然后Alice转给Bob50，Bob转给Dave120，Dave转给Alice50，Dave转给Charlie100，Charlie转给Bob80，Bob转给Dave100。整个转账过程如图所示：

这些交易之间经过清算，结果就是：

尽管转账的过程非常复杂，但是只需要在链上记录下来每个时刻的账户状态（就是每个时间段的清算结果），最终结果与所有交易信息都记到链上效果是一样的。区别在于从链上的数据并不知道交易发生的真实情况。

除了这个区别以外，还有一个重要的区别：在链外交易时，提供这些链外交易服务的组织或机构的信用与整个公有链的信用是有差别的。在链外交易时，这些交易已经不是一个去中心化的交易了，而是一种局部的中心化的交易系统。当然，由于定时会把交易清算结果写回链上，一旦结果写回链上后，我们就能够确认提供链外交易的组织是否存在篡改数据的情况了。

从经济学角度上看，小额交易由于额度较小，对于链外交易的服务商来说，篡改数据带来的利益要小于持续提供服务带来的盈利。因此，小额交易转移到链外进行，

从信任角度来讲，没有过于明显的区别。因此，未来公有链的发展趋势很可能最终变成一个类似央行清算中心的一个服务提供者，而实际上大量的小额交易只需要在链外交易中进行即可。

OK，关于比特币小额和比特币大额的内容到此结束了，希望对大家有所帮助。