本篇文章给大家谈谈虚拟货币交易造假，以及虚拟货币是骗局吗？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

数字化货币出来后，会有假币吗？

首先，央行数字货币其中一个显著特点就是可以溯源的，来源和去向都会一目了然，加上支付实名制的覆盖，无论经历多少次的流转，都可以层层抽丝剥茧找到最终流向，理论上来说比不记名的纸币要更安全。

央行数字货币功能属性与纸钞完全一样，只不过是数字化形态。用于部分取代现有的M0货币，减少伪钞风险。

虚拟货币是骗局吗？

我的观点是，没有政府信用为背书支撑的虚拟（电子）货币，都是不可靠的；在这个基础上的货币交易很大概率上都是一种不可持续的骗局---头条上众多的个人视频就有不少因为参与这种炒币行为而负债累累的，你很容易搜得到。

大约最早开始被大家广为知道的虚拟货币是08年11月网名叫“中本聪”发行的比特币（Bitcoin），它是一种P2P形式的加密数字货币，与传统意义上的法定货币不同，它依据特定算法，通过大量计算产出，P2P的去中心化特性与算法本身可以确保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；但由于设计上的限制，导致了其数量上具有稀缺性（即使可以被拆分从1枚到0.0001枚）。币的数据性真实单一存在、无法造假且具有了交换商品的价值，让它在08年金融危机下政府信用力受到挑战的情况下登上了货币市场的舞台；再后来因为其稀缺性导致了价格的暴涨暴跌，一时火了起来，甚至成为了某小国（萨尔瓦多）的法定货币。但是，从该币出生到现在已近13年了，在其与各主要法定货币的兑换价格上，依然是上窜下跳的。可以说，其真实但也风险极大，不适合我们这些普通中小散投资客、老百姓去关注并交易的。

所谓的虚拟货币的欺骗性、风险性就是由比特币大火之后引发的虚拟币风潮带来的

；虚拟货币目前已经是数不胜数，至少成千上百了。

为啥说它欺骗呢？因为虚拟货币没有了货币的特点、属性。货币的本质是度量价格的工具、购买货物的媒介、保存财富的手段，是财产的所有者与市场关于交换权的契约，本质上是所有者之间的约定。一、市面上的各种虚拟币，价值波动大，那么就没办法度量商品的价格，没法保存财富；拿它去交易普通商品的时候，其他人不认识、不信任它的真实性和价值稳定性，那它就只是个概念，丧失了作为货币的功能。既然它不是货币，一文不值的，那你拿RMB去买它，然后在平台上跟别人炒来炒去，不是骗人是什么！二、在无可靠价值的基础上，虚拟币的繁荣需要不停有人接盘，没人接盘就会币值崩塌。这有点庞氏骗局的味道了。市面上的大多数虚拟币都没有被很高明的设计，只是某种计算机技术简单加工，在你这里是个宝贝，在操盘者手里就是个数字；也没有以任何有价值的物品作链接价值锚定，因此投资它就是个去参与一个庞氏骗局，害人害己。

目前我国已经加强了对虚拟货币交易平台的管控，也推出了我们自己官方的基于政府信用为背书的可靠的货币。同样都是可靠的算法技术，同样的便捷安全，希望我们小老百姓的不要参与炒币行为了。如果想投资了，长线去持有一只股票也是可以获得丰厚回报的；也还有众多的正规投资渠道可供选择。

珍爱家人，就远离币圈、远离赌博吧！

人民币，美元，可以造假。比特币等电子货币就不可以造假吗？

问可不可以造假，先了解比特币的机制哈哈，来自李永乐老师视频比特币是一种电子记账系统，但是它的所有记录都是公开而且匿名的，这样比特币就面临几个问题，它是如何去解决伪造记录、双重支付和篡改记录的问题呢？1、伪造记录的问题我们必须保证每一条记录都是由比特币持有者所发出的，而不是由其他人伪造的。传统的记录认证方式有哪些呢？人脸识别，我们去银行办业务，银行要求我们必须本人去。签名，我们可以在某个文件上签字，表示我们认可这份文件了。指纹，每个人的指纹不一样，你按了手印就表示这件事是你认可的。这些方式在电子支付系统上都不能实现，为什么呢？因为无论是人脸识别、签名还是指纹，我利用计算机系统都可以拷贝，我可以拷贝下来你的签名，添加到我伪造的记录上。所以我们必须对这种传统的身份认证方式进行更改，这样就引入了电子签名，一个比特币的用户在注册的时候，系统会生成一个随机数，然后通过这个随机数它会产生一个叫私钥的字符串，这个私钥又可以产生一个叫公钥的字符串，私钥和公钥是对应的，同时又可以产生一个地址。这个私钥必须保存好，它是你私有的保密的，如果你的私钥丢了，那你的所有比特币就都不见了。公钥和地址都是公开的，如果你想要别人给你钱的话，你就把你的地址告诉他就可以了，如果你想给别人钱的话，你要把你的公钥和地址一起发送过去，通过公钥也反算不出私钥，私钥到公钥可以算，公钥

到私钥是算不出来的，这也是一种加密手段。私钥可以对一串字符进行加密，公钥可以把这个私钥加密之后的数据进行解密，加密和解密钥匙不一样，这种加密方式我们称之为非对称加密。最典型的非对称加密就是RSA加密，比特币也使用了非对称加密，加密的时候使用私钥，而解密的时候使用公钥。只有你能够加密，而其他人都可以解密你加密之后的信息。假如有一个人A想付给B10个比特币，他该怎么办？A首先写一条记录，A付给B10个比特币，写完这条记录后，他把这条记录进行数字摘要，也就是哈希运算，通过SHA256算法算出来的摘要，之后他通过自己的私钥进行加密，加密后产生一个密码。然后他对全网进行广播，他首先把A给B10个比特币这件事进行广播，同时他要把自己的公钥广播出去，同时他还要把上述产生的密码也广播出去，别人怎么去验证这条广播的真实性呢？首先其他接受到这条消息的人会对这条消息做哈希运算，得出一个摘要1，这个摘要其实和A算出的摘要是完全一样的，同时利用公钥和密码进行解密，用公钥就可以解密一条信息，他解密出一个摘要2，他会把摘要1和摘要2进行对比，如果相等，那么这个密码是符合要求的，这个密码符合要求，是因为你有唯一的私钥，所以你可以进行加密，我就认为这确实是A的广播。如果摘要1和摘要2不一样，说明这条消息是伪造的，于是所有用户都会拒绝这条消息，这样就保证了所有A发给B的消息都是由A签发的，这种方式我们就称之为电子签名，其实我们银行卡很多的时候也是利用这种方法进行签名的。2、双重支付的问题A要给B10个比特币，但A根本没有10个比特币，那该怎么办？或者说A有10个比特币，但他同时发了两条消息，一条是给B10个比特币，一条是给C10个比特币，这个时候别人又如何去鉴别?我们如何对付双重支付？首先说一下如何进行余额的检查。区块链是把很多的交易信息，一个块一个块打包，再把它穿一个串链起来的，而且每个人在使用区块链比特币的时候，他都会下载所有的信息，从第一个创世纪这个块开始，一直到后面所有的信息他都知道，A付给B10个比特币，并且广播出去，别人接受到这个信息就会去检查，就会去找A的比特币是从哪来的？比如A通过挖矿获得了50个比特币，A已经支付了20个比特币，这样其他人会算，获得50，支付20，还剩下30，所以A付给B20个比特币这件事是可以的，于是这条消息就会被网络所接受，如果A付给B60个比特币，那么别人会拒绝这条消息，因为它不会被确认，所以你发出去也没有用。什么时候被确认呢？直到你这条消息被别人接受了，并且打包到新的块里了，那么就算这条信息被确认了。所以这样就可以解决余额的问题，方法就是通过追溯。比如生活中有这样一种人，他卖房子了，结果卖房子时他同时跟两个买家签约，他把这一个房子卖了两次，这就叫双重支付。同样在比特币上也存在这个问题，假如有一个人A，他本来就有10个比特币，他几乎同时发了两条消息，第一条消息是A付了10个比特币给B，第二条消息是A付了10个比特币给C，那么这会有什么结果呢？网络上每一个接收者，接收到A的消息之后，都会去算，A的余额还够不够，如果有人先接收到第一条消息，那么再接收第二条消息，他就会拒绝，因为每个用户接收到A的消息之后都会去追溯，看一看A的余额够不够，所以有些人可能会先接收第一条消息，自然的就会拒绝第二条消息，因为他的余额不够了。也有一些人可能会先接收到第二条消息，这样他自然会拒绝第一条消息。此时，接收到了也没有用，因为他们会把这个消息

打包到自己的块里，此时还没有确认呢，那什么时候确认呢？在接收第一条消息的用户中，直到有一个幸运儿，找到了那道数学题的解，然后打了一个新的块，把这个块链接到当前块的后面，这样一来，这条消息就会被确认，这条消息被确认之后，刚才打包了第二条记录的这些人，一看有了新块，于是所有人都会放弃自己这个块，转而所有人都会站队，接收第一条消息，也就是说上面这条消息被确认了，而第二条消息就会被抛弃。同样道理，如果接收到第二条消息的用户中有幸运儿，成功挖矿，那么这条消息就会被确认，第一条消息就会被抛弃。所以当我们接收别人的付款时，我们不能当时就认为钱已经到账了，我们必须等着，等到这个块已经形成了，我们这条消息已经被记录到这条主链上了，我们才能认为，钱真正打给我们了，这就是我们如何防止双重支付的问题。3、防止篡改的问题有一个想篡改记录的人，他不可能伪造别人的签名，因为签名是不可伪造的，但是他可以删掉某一条记录，比如说他本来付给了别人10个比特币，现在他想把这个记录删掉，那我们怎么防止这件事？比特币有个原则，叫最长链原则，一个区块链，下面有很多矿工拼命的找方法打包新块，几乎同时有两个矿工，分别找到了一个新块，然后把这个消息广播出去，广播之后，有些人看到矿工A的消息，有的人看到矿工B的消息，这两拨人先不管，按照各自接收到的新块继续算下去，如果看到A消息的有幸运儿又挖矿成功了，这样A那伙人的人链比较长，广播消息后，另一伙的人就会重新站队，跑到A那块去，刚才挖矿的矿工B就挖矿失败。A支付给B10个比特币，他现在不想要这条记录了，他想给它抹掉，该怎么办？他可以通过这样的一个方法，他重新计算，重新打包，这个工作量是很大的，全世界一起算，每10分钟出一个，但是作为一个个人想改掉这个东西，那你就要自己算出来，算出来之后，重新打包，于是造出来一个支链来，这个支链里不含有A给B10个比特币这条信息的，你伪造了，伪造了之后别人不承认，因为这条链不够长，于是你在这个上面继续往下算，直到你算的比别人全世界算的还要长了，那么全世界的人都会认可你，于是你伪造成功了。理论上来讲你是可以进行伪造的，但问题是改动了之后，别人不承认，除非你的计算能力超过了世界上其余所有的人，万一就有这样一个坏人，他控制了全世界50%以上的电脑，就为了改掉一个区块链的记录，如果一个人有很多钱的话，他就不会去甘当一个小偷，同理如果一个人能控制全世界50%以上电脑的话，那么他不会去通过这种办法就为了抹掉自己的一条记录，他为什么不在这条真正链上努力的挖矿，让自己有更多的钱。所以从这个角度上来讲，比特币就是通过这样的方法来防止篡改的，就是说你一旦想篡改，就是跟全世界的人进行对抗，这件事其实可能性是非常低的。随着后续链的增加，你改动的难度是越来越大，所以一般大额的交易都要多等几个块，比如说等6个块之后，我们就认为基本上没有可能进行篡改了。补充共识算法：PoW：比拼算力，算力越强越容易拿到写区块链的权利；PoS：比拼财力，占的股份越大（币龄越高），越容易拿到记账权；DPoS：引入了受托人，由投票选举出的若干信誉度更高的受托人记账，受托人每隔一定周期调整，更加安全和去中心化。这些算法在许多的区块链中被广泛使用，这些算法是区块链安全的基石。4、总结比特币作为一种技术手段，是非常创新的，比特币没有一个中心发行机构，不用担心主权危机，比特币总量固定，不会存在滥发的风险，比特币天

生具有防伪属性，而且可以追溯，比特币交易的时候，手续费非常低。由于有这么多优点，有人甚至提名中本聪应该获得诺贝尔经济学奖，但是又因为比特币是一种匿名的货币，它在进行交易的时候只需要一个公钥和一个地址，你又不知道这个公钥和地址到底是谁的，所以就给很多犯罪分子提供了可乘之机，比如有人利用比特币进行敲诈，贩毒，洗钱等这样的活动，也受到了一些政府部门的打击，还有一些人把比特币当做一种投机手段，比特币暴涨暴跌，造成了许多人一夜暴富，也有许多人倾家荡产，大家应该把比特币看成一种技术手段，如果要购买比特币，也要从投资而不是投机的角度，因为从长期来看，任何一种投机行为，都会使你倾家荡产，只有投资才能使你稳定的获益。

比特币为什么不能造假

比特币是虚拟币，没有发行机构。

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保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。这同样确保了货币所有权与流通交易的匿名性。比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个。比特币可以用来兑现，可以兑换成大多数国家的货币。使用者可以用比特币购买一些虚拟物品，比如网络游戏当中的衣服、帽子、装备等，只要有人接受，也可以使用比特币购买现实生活当中的物品。

文章分享结束，虚拟货币交易造假和虚拟货币是骗局吗？的答案你都知道了吗？欢迎再次光临本站哦！