最新数据显示比特币流通市值1700.46亿美元，占全球总市值的58%，流通总量为1843.33万，24小时成交额高达60.29亿美元，至截稿为止，比特币价格为9224.04美元，相信看到这样的数据，投资比特币的人只会增多而不会减少，不过对于币圈新手来说，最为担心的问题就是投资比特币靠谱吗？以及投资比特币风险大不大？接下来小编就来给大家详细剖析一番。投资比特币靠谱吗？投资比特币是靠谱的，比特币网络及其代币使人类历史上社会经济制度最高形式的产权得以实现。一、产权新时代这是比特币的关键创新：它将产权与法律体系和暴力垄断分开。我们第一次可以拥有不依赖地方当局执行和保护的财产。隐藏，保卫，分散，移动和验证都很容易——所有这一切都可以让您获得最高级别的个人自主权。产权过去主要依赖于社会机构堆栈的其他层面，特别是对暴力的垄断和法律制度。如果此堆栈的底部不稳定，则无法拥有强大的产权。但由于比特币完全独立，它可以为世界上任何人带来最高水平的产权，无论其所处的基层机构，政府或法律体系的质量如何。比特币解锁了价值的不同维度。就像船只解锁水上运输和飞机解锁空中运输一样，作为第一个原生的数字资产的比特币解锁了一个新的备用层来存储和移动价值。比特币的所有属性都来自于这一点——它仅存在于数字世界中。因此它不会像其他资产那样在物理空间中受到攻击。这种影响只会随着时间的推移而显露出来，但我们已经可以推测出比特币将在以下方面非常有用：1.生活在产权保护薄弱地方的人2.任何受到现有金融体系歧视的人3.生活在当地货币疲软，通货膨胀(风险)率高的地方的人4.任何想要存储或移动数额可观的价值的人(越高的价值需要越高的安全性)使用比特币能使这些人更有效地合作，提高生产力，从而实现繁荣。它使他们能够为未来存钱，建立可投资于更具生产力的企业的资本，让他们与世界各地的其他人一起参与全球贸易。二、竞争带来发展比特币也可以使那些从未使用过它的人受益。作为对冲央行错误的一种手段，它使全球金融体系更具弹性。具有讽刺意味的是，它还可以改善世界各地的其他货币和财产制度。什么?是的，这就是竞争对市场的影响。如果您是Apple的客户，您将受益于三星发布新手机，因为它迫使Apple提高其产品质量以保持竞争力。因此，我们可以看到货币和产权系统的明显改善，因为比特币打开了竞争的大门并创造了一个市场。这也影响了我们对比特币不是什么的理解：VISA或PayPal的竞争对手。它与地方政府，法律系统和产权竞争——现有堆栈的基本层——而不是与其上的支付处理器竞争。文明通过合作进行扩展，但陌生人之间的合作本来就很难。社会机构可以解决这个囚徒困境，并允许我们进行更大规模的合作。在最底层，我们需要一个稳定和向善的暴力机器，执行法律制度的各项条款，建立产权制度。到目前为止，在地方政府无能的地方不可能建立强大的产权制度。比特币不以任何方式依赖现有系统，无论我们是谁无论我们在哪，都可以为我们提供最高级别的产权。三、暴涨千万倍比特币不仅仅是一项持续的技术和社会经济实验，更是一项绝佳投资，这也是它最吸引大众的地方。说起投资比特币，它亮眼的投资回报率不得不谈!比特币2009年刚出来的时候1美元可以兑换大概1300枚比特币，也就是1枚的价值是0.00076美元。如今1枚比特币接近9000美元，意味着10年翻了1100多万倍!那个时候的确夸张的像是个骗局，在加密数字货币领域，你永远不会感到平淡无聊，因为这个市场在以光速前进并且每天都在不断增长。

在各个行业的投资中，加密数字货币的投资回报率是最高的，以至于让很多最初持怀疑态度的参与者也加入了进来。想象一下，如果你在2011年投资了1000人民币，那么你现在已经财富自由了。当然，没有人能保证固定回报，但不可否认，比特币逐渐成为很多人的共识，它接下来的价格一定会比现在更贵，所以说加密数字货币是可以重点考虑的投资项目。比特币交易新手入门教程：

1.一旦一笔比特币交易被发送到任意一个连接至比特币网路的节点，这笔交易将会被该节点验证。如果交易被验证有效，该节点将会将这笔交易传播到这个节点所连接的其他节点;同时，交易发起者会收到一条表示交易有效并被接受的返回资讯。如果这笔交易被验证为无效，这个节点会拒绝接受这笔交易且同时返回给交易发起者一条表示交易被拒绝的资讯。2.比特币网路是一个点对点网路，这意味着每一个比特币节点都连接到一些其他的比特币节点(这些其他的节点是在启动点对点协议时被发现的)。整个比特币网路形成了一个松散地连接、且没有固定拓扑或任何结构的“蛛网”——这使得所有节点的地位都是同等的。比特币交易相关资讯(包括交易和区块)被传播——从每一个节点到它连接的其他节点。一笔刚通过验证且并被传递到比特币网路中任意节点的交易会被发送到三到四个相邻节点，而每一个相邻节点又会将交易发送到三至四个与它们相邻的节点。以此类推，在几秒钟之内，一笔有效的交易就会像指数级扩散的波一样在网路中传播，直到所有连接到网路的节点都接收到它。3.创建账户比特币创建全部是匿名账户，在比特币中其实所谓的账户就是用非对称加密算法(比特币使用的椭圆曲线算法)创建的一对秘钥，分为公钥和私钥。首先私钥是一个随机数，随机选取一个32字节的数，然后再使用椭圆曲线加密算法(ECDSA-secp256k1)对这个私钥压缩生成公钥。 也就是说比特币的账户本质上就是一个随机数而已，没有其他任何信息了，这也就为后来有人利用 比特币洗黑钱带来了前所未有的便利性。所以私钥一定要安全保管，不能让其他人知道，它是你拥有比特币的唯一凭证。公钥是可以暴露给别人的，事实上我们
通常发送给别人的钱包地址就是公钥通过一系列的 hash
计算和Base58编码得到的。但是钱包地址不等于公钥, 因为以上过程全部是不可逆的，也就是说你不能通过钱包地址推算出公钥，也不能通过公钥反推算出私钥。其实从私钥到地址，中间经过了9个步骤的计算处理，所以私钥是绝对安全的，不可能 被破解。4.发送交易假如有A, B 两个账户,
他们的账户信息分别如下：A私钥，公钥，地址=>

address为：private-key-A, public-key-A,0xxxxxxB私钥，公钥，地址=>

address为：private-key-B, public-key-B,0qxxxxxxx假设 A 要给 B 转账5个BTC,则付款方会发送这么一笔交易，在实际发送交易之前，A 还需要对交易进行签名，以便于其他接收节点来验证交易。由于非对称加密算法一般一次加密的数据长度有限制(一般是1024字节)， 所以在签名之前先会使用 hash
计算得到交易的摘要，然后再对交易摘要进行签名，这样也可以节约计算资源。

假设得到摘要信息是： Lsdjdxcjndjsjsdsdbck，接下来再用 A 的私钥对摘要进行签名signature = sign(summary, private-key-A) ->

"签名后结果"签名之后付款节点就会把交易广播到全网节点：我给 B 转账了5个BTC, 大家快来确认. 广播的信息包含了交易原始信息和签名信息.当然，上面是模拟主要数据，实际交易包含的信息还要多一些，下面贴出比特币的真实交易数据结构：付款方的签名付款方的资金来源的交易ID(也即上一个入账区块ID)交易金额收款人地址收款人的公钥时间戳。5.验证交易其他比特币节点收到广播交易之后会对交易进行验证，主要是验证交易是否是本人发起的。因为私钥只有本人才有，所以只要验证签名信息是 是否正确，即是否是使用私钥签名的。当然在真实交易的时候还做一些其他验证，比如付款方的 UTXO(其实就是余额)是否足够等。6.存储交易在交易验证通过之后，当前节点就会把交易写入账本，然后广播到与它相连接的节点，其他节点又会对交易进行验证，打包，广播 直到全网节点都确认了交易，B用户就会收到A发送的5个比特币。通过以上介绍，相信大家对于投资比特币是否靠谱有所了解。众所周知，比特币几乎是币圈新人的必经之路，毕竟整个币圈的沉浮，都要看比特币的脸色，学会做好比特币的投资，后面再做其他虚拟货币只会更加得心应手。即便如此小编还是要提醒投资者，投资有风险，投资需谨慎，不要盲目跟风投资。