比特币在设计理念上试图避免现有货币的诸多缺陷，这也是它备受关注的原因。但比特币的全新特征也引发了一系列全新问题。我们将逐一分析比特币的独有特征。

首先，比特币成功地实现了去中心化的货币发行与管理方式。现有货币基本上由央行发行，由一国政府用财政实力担保，这种货币发行与管理方式存在如下缺陷：其一，难免存在多种国别货币，各种货币之间通过外汇市场来兑换，显著提高了国际贸易与投资的交易成本；其二，一旦出现一国政权动荡等意外事件，该国政府发行的货币就会面临巨大的信任危机；第三，货币发行的中心化能免会产生特权，由于货币当局能够轻松征收铸币税，这可能引发货币当局短视自利的机会主义行为。相比之下，比特币在设计之时就致力于去中心化。为解决信用问题，一方面，比特币使用了一套密码学算法，使得参与比特币主区块链构建的所有用户都必须付出相当的努力才能证明其信用；另一方面，比特币产生的过程受到全网的监督，要想骗过全网所有其他用户，需要巨大的计算能力。这从技术上而言并不现实。换言之，比特币成功地利用密码学手段，解决了货币在去中心化发行时面临的信任问题，从而使得比特币的发行不需要依赖任何政府或机构，并且与互联网的去中心化特点高度吻合。

其次，比特币是一种高度匿名化的货币。其匿名性主要体现在以下三个方面：其一，比特币账号仅仅是一串数字地址，通过它无法得知拥有者的任何信息；其二，比特币账号的生成过程无需任何实名认证，账号拥有者只能通过私钥证明其所有权；其三，同一拥有者的不同账号之间没有任何关联，这意味着其他人无法得知特定用户的全部比特币持有量。然而，比特币的匿名性是一把双刃剑：它虽然通过技术手段保障了个人财产的私密性，但也为洗钱、贩毒等非法交易提供了天然的温床。此外，匿名性的另一个潜在问题是会影响削弱政府的征税能力。当前全球税收体系主要依靠监控银行账户的变动来防止逃税，这是一种基于账户实名制的有效办法。若一旦资金流动完全匿名化，征税的难度将会显著上升。

再次，比特币交易具有完整的可追溯性。对任何一枚比特币而言，其从被挖矿生成到当前所经历的全部状态，都被完整地记录在主区块链中。任何特定账户的全部交易也可以被全程追溯。最为重要的是，追溯过程并不需要认证，任何人都可以对任何账号进行查询。这有助于实现全网的互相监督以保障公平透明的市场秩序。

第四，比特币交易具有不可逆性。每笔交易只有成功和失败两种状态，而不

允许撤销操作。这种设计的初衷是为了防止付款方利用撤销操作来侵害收款方利益，以及防止退款时因需要重新建立信任关系而额外收集个人信息。针对比特币的不可逆性，存在两种截然相反的看法。支持者认为这种设计可以有效地防范信用风险，而反对者认为人难免后悔或犯错，因此不可逆性会降低比特币被广泛接受的程度。

第五，比特币的最终总量与生产速度都是事先确定的。如前所述，比特币的生产速度每 4 年减半，并将在最终达到 2100 万个。支持者认为，这种货币发行模式可以防止滥发货币以维护币值稳定。然而反对者的批评包括：其一，比特币的发行速度逐渐下降且不可调整，这将导致持续的且不断强化的通缩压力；其二，比特币增长速度的下降会形成稳定的升值预期，从而导致人们倾向于持有比特币而不是用其进行交易。这会使得比特币的交易数量日益减少、货币的流动性不断下降；其三，比特币的价值逐渐递增，可能会加剧社会分配失衡。因此，总量固定和增速递减对比特币而言既是突出的优势也是致命的弱点。

第六，比特币面临巨大的融资难题。无论是直接融资还是间接融资，均需要以借款人的身份和信用信息作为风险评价依据。但对比特币而言，搜集用户信息与其设计理念是相违背的。此外，为降低搜寻交易对象与撮合交易的成本，借贷双方需要依赖银行或债券市场之类的中介机构，这就必然导致中心节点的出现，而中心节点与比特币的设计理念也是不相符的。这意味着尽管比特币融资在技术上是可行的，但这将会破坏比特币的设计初衷。融资难题将成为比特币发展的重大阻力。

第七，比特币既不存在货币乘数，也无货币政策可言。既然无法利用比特币融资，这就意味着比特币没有其他货币均拥有的货币乘数。这固然有助于控制通胀，但也导致比特币难以满足市场的流动性需求。此外，比特币也不存在货币政策的概念。比特币的发行无需政府，这从技术上限制了政府可能对其进行的干预。鉴于比特币的特殊性，基准利率、准备金率与公开市场操作等传统货币政策工具对其而言均是无效的。比特币的这一特征虽然能够避免过度的宏观政策波动以及维持币值稳定，但也排除了通过货币政策进行宏观调控的可能性。

第八，比特币是天然的全球性货币。比特币既没有国界，也无需兑换。比特币作为全球性货币的积极一面是有助于降低国际贸易与资本流动的交易成本，而消极一面可能加剧局部危机的传染、放大全球的系统性风险。