

根据中本聪的构想，比特币要建立的是一套“完全通过点对点技术实现的，在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何金融机构”的电子货币系统。在中本聪看来，利用密码学的知识，可以有效代替第三方机构提供的信任，从而实现这样的构想。