

一、比特币是什么,有哪些特点？

一种P2P(点对点)形式的虚拟货币。去中心化的记账系统；

去中心化：任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护、共同管理；

开放透明性：系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

自制性：人为不可干预，决定得超过一半的人去做；区块链采用基于协商一致的规范和协议（比如一套公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

信息不可篡改特性：一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

匿名性：由于节点之间的交换遵循固定的算法，其数据交互是无需信任的（区块链中的程序规则会自行判断活动是否有效），因此交易对手无须通过公开身份的方式让对方自己产生信任，对信用的累积非常有帮助。

可溯源性：因为公开透明和不可篡改的特性，所以每一笔交易信息都可以追溯其来源！

二、比特币原理

数据存储在网络节点里，比如每一台电脑里；那么问题来了，数据在每一台电脑里，已谁的为准，数据被篡改了怎么办；

1.数据的验证

假如说如下数据：