比特币使用的核心技术：哈希技术，构建区块链，保证交易不被篡改

数字签名技术，确保正确交易

交易的要求：1.花钱前证明自己有钱（数字签名）

2.花钱时将钱打入指定账户（数字签名）

3.输入输出交易单不可篡改（区块链）

区块链：

区块包含头部和账单，构建一个新的区块链的头部要包含前一个区块链的头部、账单等信息以及一个随机数的信息，首先将前一个区块链的头部、账单等以及一个随机数进行两次sha256计算得出哈希值，要求这个哈希值的前n位是0，由于要求的n值一直在变，包含的上一个区块的信息也不相同，这个随机数要靠计算机不断计算得出，概率为1/2^n，谁先试出这个随机数，谁就构建了新区块。

构建新区块可以获得比特币奖励，也就是所谓的“挖矿”，比特币奖励是这个系统的激励机制，在系统内部的交易只能通过比特币进行，而比特币的获取方式除了别人转账就只有靠挖矿获得。同时比特币的奖励数量会以四年为周期逐步递减，越早挖矿的人获得的越多，因此大家都踊跃挖矿。

如果两人几乎同时构造出了新区块，那就要看后续两个分支链哪个更长，系统遵循最长链原则，选用链条更长的那个分支，另一条短分支不被承认，上面的交易也无效，所以后来的矿工会选择将新区块建立在更长的链条上，保证区块链一直延续下去。

由于每一个区块链包含了之前所有区块链的信息，所以区块链中的信息无法更改。如果有人试图修改交易信息，那他就要从被修改的区块开始，单枪匹马构造出更长的区块链取代以前的链条，但由于构造区块是有比特币回报的，全世界都在争着构造新区块，所以以个人的力量很难开出一条新区块。

数字签名技术：

采用非对称密码技术。

个人注册之后会得到一个私钥，一个公钥，一个地址，私钥仅自己可见，公钥和地址公开，公钥相当于账户，私钥相当于自己的钱包，私钥经过椭圆曲线加密和两次哈希计算后可以得出公钥，公钥不可以得出私钥。

UTXO（Unspent Transaction Output）：生成于一笔针对自己钱包的交易。

账户余额：因为比特币是系统内部产生的，所以每一笔钱的交易都有记录。追溯和自己钱包有关的所有UTXO，从获得第一笔比特币开始，计算所有输出输入，得出余额。

假如A转了10比特币给B：

1.A首先要使用自己的私钥解锁之前的UTXO，证明自己钱包里有足够的余额支付。

2.A使用B的公钥锁定这个10比特币的输出，形成UTXO，并对此交易进行广播。

3.B确认收钱，要用自己的私钥解锁A转账给B生成的UTXO，并且发送给记账节点认证，如果大部分认证通过，这个交易就是有效的，A失去10个比特币，B得到10个比特币。

问题：

1. 上面A转账给B的流程，不确定是不是这样，记账节点是根据A的广播进行验证的吗？
2. 梅克尔树的校验：为什么只要知道自己的数据就能算出这个数据有没有被篡改有没有在区块内？（图中绿色线的数据是怎么来的？）