3.账户余额在哪

#如何证明自己拥有这么多钱

首先，john一共有9块钱，当它没有被使用的时候，它会被标识为utxo（Unspent Transaction Output),当一旦引用它的时候，就会变成Spent Transaction Outout

通过上一次交易的哈希来证明自己拥有还这么多钱，例如上一次当中

{

input:{

txid=这个地方引用上次交易，实际使用哈希

vout=这是试图使用的UTXO

ScriptSignature=John的数字签名

//transactionid(这一地方上一章存在空缺)

}

output:{//接收方Bob的信息

amount=5;

script PubKey=Bob的公钥;

}//这个地方可以验证是本人

}

#那么如何证明自己是john呢?

UTXO签名包含它的私钥，比如加密“hello”必须使用私钥来生成signature（这个会公布）

如果真的是John想要发送，那么使用UTXO中John的公钥，可以将Signature进行还原并与之前公布的进行比对（这个是用于别人来验证的）