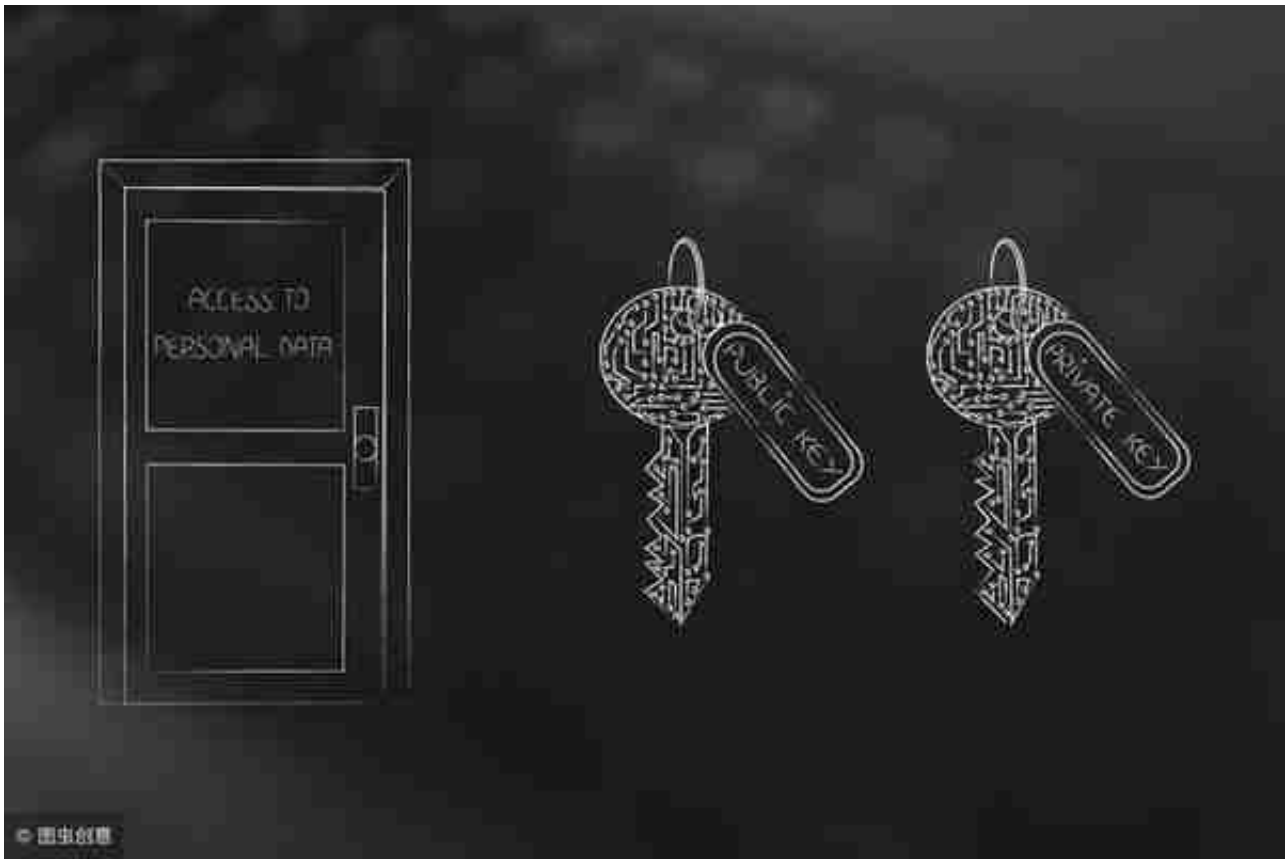
如果说2015年在香港举行的“比特币扩容研讨会”上最令人兴奋的提议，那毋庸置疑是开发者Pieter Wuille博士提出的隔离验证（Segregated Witness）。这个提议受到技术界人士的好评，隔离验证有望能改善比特币的性能表现，而有些人甚至希望它能提供一种扩容的解决方案，帮助比特币社区恢复一定的和谐。



签名是怎么来的？

为了证明对应于与比特币地址的私钥的所有权，理论上可以在交易的scriptSig中包含私钥，但是这样一点都不安全。最重要的是，任何看到交易的人都可以获取私钥，并创建一笔新的交易（或更改原始交易），将原始交易中的接收方改成自己。如果真是这样的话，对矿工而言偷比特币就会是小菜一碟了，因为他们是挑选交易进行确认的人。

因此，scriptPubys通常要求scriptSig包含一个或多个签名来解锁比特币。

签名是一种密码学技巧，使用私钥与任意其他数据组合来计算出唯一的数字字符串。并且，根据密码学原理，可以使用对应的公钥来验证签名是不是使用该私钥创建的。因此，签名既证明了私钥的所有权，又证明了该私钥的所有者对特定数据片段的批准，同时不需要泄露私钥。

在比特币中，私钥通常用于对交易数据进行签名来减去交易输入。（包括，script PubKeys、锁定的数量和一些其他细节。）随后，将签名和用于使用比特币的公钥添加到交易的输入字段中。这样也证明了私钥的所有者确实打算创建交易并确保它不会被篡改。

然后，将所有这些交易数据（包括此时的交易输入）一并哈希运算，创建出交易ID，用于标识出特定交易。如果交易随后被打包入块，那么矿工会将交易ID与另一个交易ID一起哈希运算产生新的哈希值。如果有其他两个交易ID的哈希值，则再次进行哈希处理，一直持续到只剩下一个哈希值为止。这种散列结构称为默克尔树（Merkle Tree），最终产生的哈希值为默克尔根（Merkle Root）。该默克尔根与其他区块数据组合以形成区块头（header），用于标识特定区块。最后，这个区块头的哈希值会被包含在下一个区块的区块头中，从而将区块链接在一起。

比特币被认为是不可篡改的，因为追溯性地更改任意交易的任何部分都会改变交易ID，进而改变区块头。而改变了的区块头不再符合工作量证明的要求，并且由于区块头会影响后续区块头的组成，因此它们中的任何一个都会被视为无效。