**区块链隐私保护如何解决-张馨文**

目前有混币、环签名、同态加密、零知识证明等几种方式。

1. **混币原理：**割裂输入地址和输出地址之间的关系。在一个交易中，假如有很多人参与，其中包括大量输入和输出，这样会比较难在输入和输出中找出每个人的对应对，这样一来，输入与输出之间的联系被事实上割裂。
2. **环签名：**在环签名方案中，环中一个成员利用他的私钥和其他成员的公钥进行签名，但却不需要征得其他成员的允许，而验证者只知道签名来自这个环，但不知到谁是真正的签名者。环签名解决了对签名者完全匿名问题，环签名允许一个成员代表一组人进行签名而不泄漏签名者的信息。
3. **同态加密：**同态加密是一种无需对加密数据进行提前解密就可以执行计算的方法。通过使用同态加密技术在区块链上存储数据可以达到一种完美的平衡，不会对区块链属性造成任何重大的改变。简单来说，区块链仍旧是公有区块链。然而，区块链上的数据将会被加密，同态加密技术使公有区块链具有私有区块链的隐私效果。
4. **零知识证明：** ZKP是一种密码学技术，是一种在无需泄露数据本身情况下证明某些数据运算的一种零知识证明，允许两方（证明者和验证者）来证明某个提议是真实的，而且无需泄露除了它是真实的之外的任何信息。