**·Project10: report on the application of this deduce technique in**

**Ethereum with ECDSA**

（参考：①https://blog.csdn.net/weixin\_43867940/article/details/130258535 ）

（参考：② https://learnblockchain.cn/article/5012 ）

**报告如下：**

**以太坊中的 ECDSA**

我们已经了解了 ECDSA 是怎么回事，接下来就看看以太坊中如何使用 ECDSA 对交易进行签名。

Secp256k1是指比特币中使用的ECDSA(椭圆曲线数字签名算法)曲线的参数，并且在高效密码学标准（Certicom Research，http://www.secg.org/sec2-v2.pdf）中进行了定义。以太坊也使用了 Secp256k1。

对以太坊一笔交易进行签名的大致步骤如下（简化后）：

1.对交易数据进行 RLP 编码

2.对第一步得到的编码进行哈希

3.将哈希与标识以太坊的特定字符串拼接在一起，再次哈希。这一步是为了保证该签名仅在以太坊上可用

4.用上一节介绍的ECDSA算法对第三步得到的哈希进行签名，得到 (r, s, v)，v 是一个字节，可以看这里对它的解释

https://bitcoin.stackexchange.com/questions/38351/ecdsa-v-r-s-what-is-v

5.将第四步得到的签名与交易数据拼接，再次进行RLP编码，得到最终的签名消息。

验证签名应该也很简单，这里不再赘述。不过这里有个点比较好奇，就是接收到交易的节点在验证签名时，如何获得签名者的公钥？可以参考这篇文章https://www.jianshu.com/p/6cb992091886

**因为可以从签名中恢复公钥，再从公钥中得到签名者地址，所以签名消息中的交易内容不需要包含发送者的地址。**