Project 7: report on the application of this deduce technique in Ethereum with ECDSA

参考网站

https://learnblockchain.cn/books/geth/part3/sign-and-valid.html

SEC 1, ver. 1.9 (secg.org) [47-48] [13] [11-12]

为了恢复公钥，我们需要知道椭圆曲线的参数(p,a,b,G,n,h) h为椭圆曲线点的个数除以G的阶；消息M以及ECDSA的签名(r,s)

1. 令 x = r + j * n $j \in [0, h]$
2. 将整数x转为256进制的字符串X，$len(X) = mlen$ = $(log_2 p)/8$
3. 将字符串$02_{16}||X$转为椭圆曲线上的点R
4. 若 $nR \neq O$ 重新执行第一步
5. 由M执行ECDSA签名的第二三步，得到哈希值e
6. for k in range(2):

   $$Q = r^{-1}(sR - eG)$$

   验证Q是否为公钥 若Q通过验证则输出Q

   将R变为-R重新执行
7. 若未找到相应的公钥 则输出失败