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

如交易的结构所述，交易消息不包含任何“from”字段。这是因为发起者的公钥可以直接从ECDSA签名中计算出来。一旦你有公钥，你可以很容易地计算出地址。恢复签名者公钥的过程称为\_公钥恢复\_。

给定ECDSA数学中计算的值 r 和 s，我们可以计算两个可能的公钥。

首先，我们根据签名中的x坐标 r 值计算两个椭圆曲线点R和R’。有个两点，因为椭圆曲线在x轴上是对称的，所以对于任何值+x+，在x轴的两侧有两个可能的值适合曲线。从 r 开始，我们也计算r-1这是 r 的倒数。最后我们计算 z，它是消息散列的最低位，其中n是椭圆曲线的阶数。然后两个可能的公钥是：K1 = r-1 (sR - zG)和K2 = r-1 (sR’ - zG)。其中:K1 和 K2 是签名者公钥的两种可能性。r-1是签名的+r+值的倒数。s是签名的+s+值。R和R’是临时公钥\_Q\_的两种可能性。z是消息散列的最低位。G是椭圆曲线生成点。

为了使事情更有效率，交易签名包括一个前缀值 v，它告诉我们两个可能的R值中哪一个是临时的公钥。如果 v 是偶数，那么R是正确的值。如果 v 是奇数，那么选择R’。这样，我们只需要计算R的一个值。

而ECDSA是基于 ECC 的数字签名算法，在比特币、以太坊等区块链网络中大量使用。每一笔区块链交易执行之前都必须进行权限校验，以确保该交易是由账户对应的私钥签发。256 位私钥的 ECDSA 签名可以达到 3072 位 RSA 签名的安全强度。