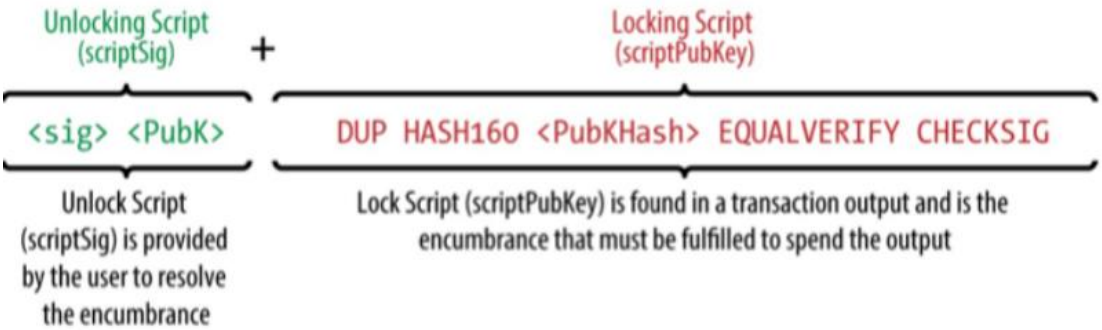
ECDSA 数字签名算法是使用椭圆曲线密码 ECC 对数字签名算法 DSA 的模拟。椭圆曲线离散对数问题没有亚指数时间的解决方法，远难于离散对数问题，椭圆曲线密码系统的单位比特强度远高于传统的离散对数系统。因此在使用较短的密钥的情况下，ECC 可以达到与 DL 系统相同的安全级别。这带来的好处就是计算参数更小，密钥更短，运算速度更快，签名也更加短小。因此尤其适用于处理能力、存储空间、带宽及功耗受限的场合。

尽量减少每一笔交易/每一个区块的大小，对于缩减区块体积，提升区块的传播速度等方面大有裨益。Bitcon 网络中一个典型的 P2PKH 交易中，解锁脚本中签名值 sig 按照 DER 编码长度大约 70 个字节，压缩的公钥 PubK 需要 33 个字节（推荐使用压缩形式），锁定脚本中字节码 DUP， HASH160， EQUALVERIFY，CHECKSIG 各占用一个字节，而 PubKHash 为 20 个字节，则下图展示的脚本占用链上存储空间大约 130 字节。



ECDSA 签名机制的一个特性是可以根据签名值 sig 推算出公钥 PubK，下文用可恢复签名来指代这一特性。这意味着解锁脚本中的 33 个字节的压缩公钥 PubK 字段是冗余的，利用从 ECDSA 签名值可以恢复公钥的特性，解锁脚本中不再需要字段 PubK，则上图所示的交易只需要占用 100 个字节左右的存储空间，大约为 23%的存储空间节省。Bitcon 利用这一特性，那同样大小的区块中可以存放更多交易，历史区块占用的存储空间也可得到大幅缩减。

实际上，为了能够从签名值恢复出唯一的公钥值，还需要存储额外的消息。对于 ECDSA 签名值中的 r≡x mod n,（x，y）∈G，x，y∈F_p，根据曲线的参数可知，当 n<p<2n，则当 x<n 时，r=x，而当 x⩾n，有 x=r+n。也即根据 r 以及 x 是否大于 n 这 1 比特的消息可以唯一确定 R=kG 的横坐标 x。进一步根据椭圆曲线方程可以从 x 的值计算出纵坐标 y 的值，y 和-y 都是对应 x 的合法值，也即根据 x 的值以及 y 为奇数还是偶数这 1 比特信息可以唯一确定点 R=kG。有了 R 信息之后，对于合法的签名可以通过如下推算公钥 P：

$$R=s^{-1}（eG+rP）\rightarrow rP=sR-eG\rightarrow P=r^{-1}（sR-eG）$$