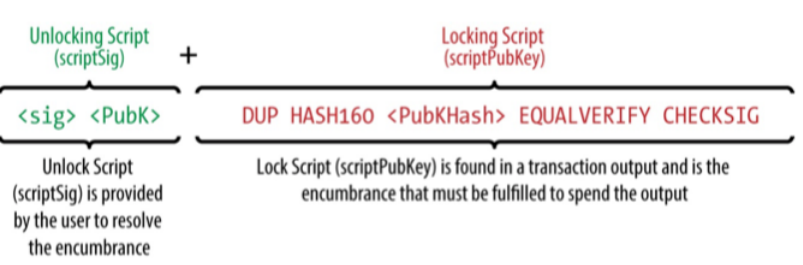
ECDSA数字签名算法是使用椭圆曲线密码ECC对数字签名算法DSA的模拟。椭圆曲线离散对数问题没有亚指数时间的解决方法，远难于离散对数问题，椭圆曲线密码系统的单位比特强度远高于传统的离散对数系统。因此在使用较短的密钥的情况下，ECC可以达到与DL系统相同的安全级别。这带来的好处就是计算参数更小，密钥更短，运算速度更快，签名也更加短小。因此尤其适用于处理能力、存储空间、带宽及功耗受限的场合。

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∈，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=（eG+rP）→rP=sR-eG→P=（sR-eG）