ZPN公链简介

查看密钥对

- 传出视图键（ovk）：256位对称密钥，通过向密钥（sk）附加2字节，计算结果字节字符串的Blake2b哈希值，并将结果截断为256位来生成。

  ovk = blake2b(sk || 2, personalization: "Money ", length: 512 bits)

- 传入视图键（ivk）：JubJub组标量字段的元素。通过将授权密钥（ak）连接到无效器派生密钥（nk）（均以压缩形式表示为仿射点），计算结果字节字符串上的Blake2b哈希值，并将结果截断为251位来生成：

  ivk = blake2s(ak || nk, personalization: b"Zcashivk", length: 256 bits).truncate(251 bits)

传输密钥

JubJub曲线上的点，通过将传入视图密钥（ivk）乘以公钥生成器生成：

pk = ivk * PUBLIC_KEY_GENERATOR