ZPN公链简介

ZPN帐户是密钥的集合。有些密钥是私有的，只有账户所有者才应该知道。密钥可以与ZPN网络中的其他参与者共享以接收交易。

ZPN账户最重要是密钥（sk），账户中的所有其他密钥都派生自sk密钥。

私钥

- 密钥（SK）：用于派生账户中所有其他密钥的私有密钥，有时也称为支出密钥。
- SPEND AUTHORIZATION Key（ASK）和Authorization Key（AK）：用于授权资产支出的私钥对
- 证明授权密钥（NSK） 和 Nullifier 派生密钥（NK）：用于派生 Nullifier 的私钥对
- 传出查看密钥（OVK）：用于解密从账户发送的交易的私钥
- 传入视图密钥（IVK）：用于解密发送到账户的交易的私钥

公钥

- 传输密钥(PK)：参与者用于将交易发送到账户的公钥。这有时也称为帐户的公共地址。