2018/04/02

Zcash中的值是透明或者屏蔽的：

转让透明价值的工作基本上与比特币一样，并具有相同的隐私属性。

屏蔽值由票据携带，票据指定金额和支付密钥（paying key）。 支付密钥是支付地址的一部分，支付地址是票据可以发送到的目的地。 和比特币一样，这与一个私钥相关联，该私钥可用于花费发送到该地址的票据; 在Zcash中这被称为支出密钥（spending key）。

Paying key ： 用来指定支付地址。

Spending key ： 用来花费票据。

票据（notes），票据承诺（note commitments）和否定器（nullifier）之间存在着1：1：1的关系。

一个交易包含：输入、输出和脚本以及零个或多个JoinSplit描述。

JoinSplit描述：