# 密码学在区块链中的应用

## 哈希函数

使用哈希的查找结构，有助于用较小的空间表示较大的集合的存在，提高空间利用率；哈希函数需要考虑到密码学安全，因此需要 *碰撞阻力* 、 *隐秘性* 和 *谜题友好* 的特性

**承诺协议**的执行便是应用了哈希函数，承诺也要满足 *隐秘性* 和 *约束性*

## 数字签名

数字签名用于证实某数字内容的完整性和真实性，用于满足比特币中的去中心化管理

数字签名有**公钥私钥**，由三个算法构成： *密钥生成* 、 *签名过程* 和 *验证过程*

数字签名的特性是 *有效签名能通过验证* 和 *不可伪造*