# 区块链技术与应用笔记

## 1．比特币中的密码学

Cryptographic hash function(加密哈希函数)

--collision resistance x!=y but H(x)=H(y) brute-force：穷举可能找x对应的y 对比上传下载的hash值确定内容是否发生改变 是否能被人为制造很重要

--hiding(单向)：x->H(x)，暂时不可被反向破解 实际中H(x||nonce)

---digital commitment(equivalent of a sealed envelope:信封预测)

--puzzle friendly 无法限定hash值的范围

(public key,private key) from asymmetric encryption algorithm非对称加密：我发信息要用对方的公钥，那对方解密之后怎么知道消息的内容呢？ A给B发信息m，用B的公钥加密m->M，B用私钥来对M进行解密。还有确认消息m的完整性，用签名与认证，A可以对hash(m)用私钥进行签名生成S,B用A的公钥进行解密得到hash1和消息，B再用相同的hash函数计算得到hash2，与hash1比较确认。