# 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

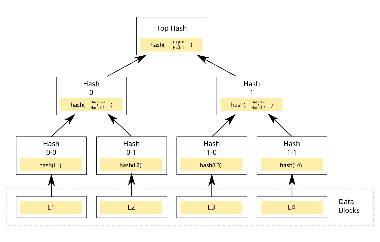
(public key,private key) from asymmetric encryption algorithm非对称加密：我发信息要用对方的公钥，那对方解密之后怎么知道消息的内容呢？ A给B发信息m， 用B的公钥加密m->M，B用私钥来对M进行解密。还有确认消息m的完整性，用签名与认证，A可以对hash(m)用私钥进行签名生成Sig，A将m和Sig一同发给B，B用A的公钥进行解密Sig得到hash(m)，B再用相同的hash函数计算m得到hash2，与hash(m)比较确认。

## 2．比特币中的数据结构

Hash point genesis block创世区块 <- H() <- most recent block 特性：tamper-evident log防篡改日志 可以从最后一个hash值向前推

块头的Hash值为上一个块的所有内容加密所得

Merkle tree

 做出的内容修改会向树根传递，叶子节点为交易

Block head ：version ；hash of previous block header；merkle root hash ；target(阈值) ；nonce

Block body ：transaction list；

Merkle proof ： 验证data block到root hash的路径上的hash值，交易是否真实有效，卖方提供 proof of membership

验证Proof of non-members ，如果交易有序，检查两个

Full node

Light node(轻结点)

## 3．比特币中的共识机制

Double spending attack 中心维护表

CreateCoin A(10) A->B(5) C(5) B->C(2) D(3) C->E(7) 有新交易时，会回溯区块链检查是否合法

铸币交易