# 基础知识考试题目

## 每题10分, 共计30分, 独立完成

## 尽可能地采用课件和教材的记号回答.

## 下半年开学前发回到我qq邮箱

姓名 学号

# 考题

1. 证明区块链具有数据库的ACID性质.
2. 马云想给马化腾发送100 BTC。请按照时间顺序描述，马云点击数字钱包发送按钮后，区块链世界所发生的事情。描述的时候，要有主语和动词。主语不得是“区块链”, 而应该细化为”矿工”,“客户端”等词语.
3. 利用下图的commitment scheme 和课件中的Schnorr’s identification protocol, 实例化一个具体的ZK协议. 要求提供: 各方的输入, 输出, 过程(即各方的每个step)

