《区块链基础》第 2 次作业

深入理解 BLS 签名，并熟悉 BLS 签名在比特币钱包中的应用，进行编程（编程语言不限）实现，并**提交程序源码、调试结果截图**。具体要求如下：

1）学习 BLS 签名的相关理论基础，形成学习笔记，并编程实现椭圆曲线哈希、双线性配对，可引用第三方程序库；

2）基于 1），编程实现不同应用场景的 BLS 签名，包括：基本 BLS 签名（1 个消息，1 对公私钥）、BLS 签名聚合（多个消息，多对密钥）；

3）【选做】编制计算机程序，模拟基于 BLS 签名的比特币钱包及安全交易。

参考链接：

https://www.jianshu.com/p/0fb609a28c38
https://blog.csdn.net/shangsongwww/article/details/89486686

提交要求：

1、请大家于 4 月 30 日截止 24:00 前提交至 23648094@qq.com

2、邮件主题格式：02_2025 区块链_学号_姓名_提交日期（8 位数格式，比如 20250422）

3、邮件附件格式：程序主文档的文件转换成 PDF 格式，再对所有文件进行打包（打包文件的命名规则同上面第 2 条）