比特币与区块链

C6.1. 为什么比特币使用基于椭圆曲线的公钥算法，而不是使用流行的 RSA 算法？

C6.2. 比特币系统中的公钥哈希长度是多少？

C6.3. 对传统 Base58Check 编码的比特币地址，若首字符是“1”或“3”，分别表示公钥哈希地址还是脚本哈希地址？

C6.4. Bob 从 Alice 的一笔交易输出中得到 5 个比特币，随后在新交易中向 Charlie 支付 3 个比特币。剩余的 2 个比特币会怎样？

C6.5. Alice 从先前交易的一个输出中获得 5 个比特币。她想用这笔钱分别向 Bob 支付 2 个比特币、向 Charlie 支付 2.99 个比特币，并为两次付款各建一笔交易。可行吗？

C6.6. 某交易输出由以下脚本锁定。（1）给出可用的解锁脚本。（2）这个锁定脚本安全吗？

```
<3> OP_MUL OP_ADD <50> OP_EQUAL
```

C6.7. 某交易输出由以下标准 P2PKH（pay-to-public-key-hash）脚本锁定。（1）谁能提供有效的解锁脚本？（2）攻击者想花费该输出，在看到别人提交的有效解锁脚本后，立即把它复制到自己的交易中。这样能成功吗？

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY
              OP_CHECKSIG
scriptSig:    <sig> <pubKey>
```

C6.8. 在 P2PKH 交易中，先前交易 T 的某个输出被当前交易作为输入消费，解锁时必须提供签名。Bob 以为该签名是对交易 T 生成的，而不是对当前花费交易生成的。若真是如此，设计是否安全？

C6.9. Bob 从 P2SH（pay-to-script-hash）输出中得到 3 个比特币。花费时，解锁脚本必须包含 redeem script，但 Bob 输入该脚本时出错了。会发生什么？

C6.10. 为接收付款，Bob 把一个公钥交给 Alice，Alice 随后向该公钥支付 3 个比特币。Bob 后来才发现自己给错了：与该公钥对应的私钥已经丢失。Bob 能要求 Alice 撤销交易吗？这 3 个比特币会怎样？

C6.11. 当矿工看到区块链出现两个分支时，应接受哪一个分支？

C6.12. 什么是交易的确认数？

C6.13. 比特币矿工有哪些激励措施？

C6.14. Bob 找到一种高效算法：对任意哈希函数，给定数值 h 和字符串 $M1$、$M2$，都能求出 R，使 $\texttt{hash}(M1\|R\|M2) = h$。这一发现会对比特币系统产生什么影响？