1.简要解释比特币私钥、公钥和地址的关系。

私钥是256位数字，可通过非对称加密算法推导出公钥，公钥在通过一系列哈希运算推导出地址。

2.比特币私钥、公钥和地址长度（原始长度，未经过base58check编码）分别多少？

私钥原始长度位256位（32字节），公钥为512位（64字节），压缩后为257位（33字节），地址为160位

3.什么是哈希函数?解释哈希函数的单向性。举例两个比特币中常用的哈希函数。

哈希函数是一种科学函数，可以将输入的任何数据转化为独一无二、任意长度的哈希值。

单向性值任意哈希值无法通过逆向运算求出对应输入数据

常用的哈希函数有SHA-256，RIPEMD-160

4.下面是两个经过base58ckeck编码的值，它们是比特币地址还是私钥？A=1AVYKXSaH8Rm9YBGjuuY9ZixqnP614AWGS

B=5HxwZhERaMvPZrNJRNfuEsBHvMhnN6GNYugVPEiR9aVNp3vmHWb

A为比特币地址

B为比特币私钥

以下题目简单回答要点，答案不要太长。

1、冷钱包与热钱包的区别是什么？

冷钱包：私钥离线存储，安全性高；

热钱包：私钥在线存储，便于交易。

2、简述随机性钱包和分层确定性（HD）钱包的区别。

随机性钱包：每生产一个新地址，要备份新的子私钥，繁琐

分层确定钱包（HD）：通过主种子衍生子私钥和地址，记住主种子就可以恢复资产

3、如果你的HD损坏了，所有的私钥都丢失了，你能如何恢复它？

通过备份的助记词和密码来恢复HD钱包与私钥

4、什么叫扩展公钥和扩展私钥。

扩展公钥：通过公钥和链码，推导出子公钥

扩展私钥：通过私钥和链码，推导出子私钥和子公钥

5、HD 钱包的父扩展公钥可以独立推导子扩展公钥，而无需依赖主私钥。这样设计的有什么应用场景？

运用到金融场景，通过扩展公钥，可以实现对资金的收取和审计账户等交易，无需暴露私钥

1、简述比特币UTXO模型。

UTXO是未花费比特币的输出。每次交易都会消耗存在的UTXO和产生新的UTXO

2、简述锁定脚本和解锁脚本概念和它们的关系。

锁定脚本是UTXO交易的条件

解锁脚本是提供满足锁定脚本的条件，解开UTXO锁定脚本。

解锁脚本提供满足的条件，它才解开UTXO锁定脚本，才能花费UTXO。

3、在比特币交易中，Alice 向 Bob 发送 10 BTC，请回答以下问题：

3.1.发送者地址（Alice 的地址）和接收者地址（Bob 的地址）存在哪？

Alice 的地址存在UTXO中。

Bob 的地址在交易输出部分，编码进锁定脚本

3.2.发送者Alice原来的钱存在哪里？

存在UTXO当中

3.3.接收者Bob 收到的 10 BTC 存在哪？

新的UTXO之中

3.4.如果Bob以后想花这10BTC（支付给C）,他该怎么做？

Bob创建新的交易，用含10BTC的UTXO作为交易的输入，用私钥创建解锁脚本解锁UTXO；并创建新的UTXO，用C的地址作为锁定脚本，把资金转给C。

1、简述比特币轻量节点（SPV）和全节点区别？

轻量节点：只下载区块头的数据，不下载完整数据。

全节点：下载整个区块链的区块和交易数据。

2、假设我们有一个简单的 Merkle 树，包含 4 笔交易（TxA, TxB, TxC, TxD），其哈希值如下：

Hash(TxA) = H\_A

Hash(TxB) = H\_B

Hash(TxC) = H\_C

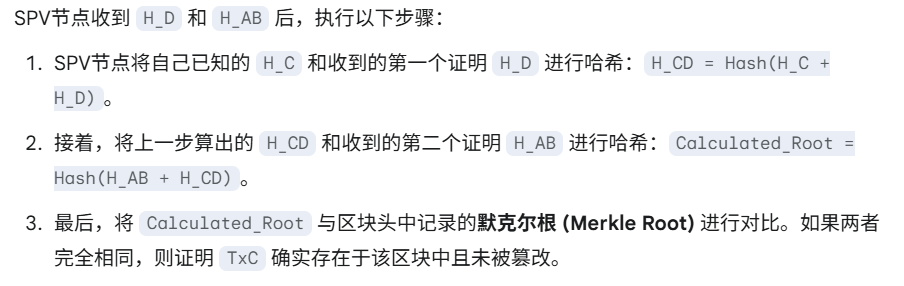
Hash(TxD) = H\_D

现在需要全节点向SPV节点证明交易 TxC 包含在该 Merkle 树中，请提供：

2.1.所需的 Merkle Proof 路径（即需要提供哪些哈希值）

H\_D,H\_AB

2.2.验证步骤（如何通过这些哈希值计算 Merkle Root，并与已知的 Root 对比）



3、简述工作量证明（POW）的工作过程。

打包交易 构造区块头 计算哈希 寻找有效哈希 广播区块

4、简述区块头中的Target值和挖矿难度的关系。​

难度值越高，目标值越低

5、比特币的 PoW 要求矿工找到一个 nonce，使得区块头的哈希值满足：SHA256(Block Header))≤Target，其中Target=0x00000000FFFF0000000000000000000000000000000000000000000000000000

5.1.如果当前 nonce 从 0 开始递增，最多尝试 1,000,000 次，旷工能否找到符合条件的 nonce？为什么？

不能。43亿次尝试才可能找到符合条件的nonce,仅100万次尝试，与所需工作量对比，成功概率极小。

1、解释临时分叉，硬分叉，软分叉的区别。

临时分叉是当两个矿工同时挖出新的区块时，区块链会分叉出两条链，但根据最长链原则，最短的那条链会被刨析，

硬分叉是不向后兼容性的协议升级

软分叉是向后兼容性的协议升级

2、当对区块链升级，将区块链大小从“<1MB”增加到“<8MB”，属于硬分叉还是软分叉？解释原因。

硬分叉。旧矿工只认同<1MB规则产生的区块是有效的，大于1MB产生的区块会被它认为无效，区块链因此造成分歧，无法团结。

3、解释最长链原则。

区块只认工作量证明最多的链为主链

4、什么是51%攻击？举例说明它如何造成比特币双花攻击。

攻击者拥有整个矿池中超过50%的算力，可以篡改已写入区块的交易，进行双花攻击和交易审查。

假设攻击者打算通过10BTC向Bob购买相应物料，当攻击者完成支付，并向区块链广播这个交易，Bob把物料交给攻击者，而攻击者突然上传了新的最长区块，这个区块中不包含已经支付给Bob的交易，所有区块都认这条链为合法链，这样攻击者10BTC依然拿在手里又得到了物料。

5、简述以太坊账户模型和比特币交易模型区别。

以太坊账户模型：账户/余额模型，类似银行账户

比特币交易模型：为未花费交易的UTXO模型

6、以太坊交易中的 Nonce 两个主要作用是什么？

防止重放攻击和保证交易顺序

7、简述以太坊外部账户和合约账户的区别。

以太坊外部账户：由普通用户控制，拥有私钥，能主动发起交易。

合约账户：由内部智能合约控制，不拥有私钥，不能主动发起交易。

8、以太坊交易中并不含有发送者地址，那么它是如何计算出来？

通过数字签名反推出来。

1、消息调用与交易的区别是什么？请简要说明。

消息调用由合约账户发出，是合约与合约之间的交互。

交易由外部账户（E0A）发出，通过私钥签署进行区块广播。

2、在Solidity中，payable 关键字的作用是什么？请简要说明。

Payable函数的作用是允许一个函数或地址接收以太币(Ether)

3、简述Solidity中的三种变量类型：状态变量、全局变量和局部变量，并分别说明其特点。

状态变量：存储在区块合约当中，gas消耗高。

局部变量：只在函数调用执行时有效，gas消耗低

全局变量：任何函数都可访问调用，提供区块和交易信息的特殊变量

4、简述 Solidity 中 call 和 delegatecall 的基本区别。

Call是合约A调用合约B函数，代码在合约B上下文执行

Delegatecall是同样调用合约B函数，代码在合约A上下文执行

5、什么是智能合约中的重入攻击？请简要说明，并举例两种常见的防御方法。

合约A调用外部合约B，恶意B回调A中函数，在A更新状态前再执行该函数，窃取A中资金。

用transfer方法不用call方法

用互斥锁

用检查-生效-交互模式

6、什么是智能合约中的上溢（overflow）与下溢（underflow）？请分别举例说明。

上溢是通过增加导致超出智能合约范围

下溢是通过做减法超出智能合约的范围

上溢如持有大量加密货币者可能因为接受小额交易，导致其加密货币清零

下溢如持有小额加密货币者可能通过减少持有量，盗取智能合约中大量的加密货币

1、小王计划开发一款区块链游戏，正在考虑游戏内通用货币应使用加密货币（如ETH）还是发行代币Token。

（1）加密货币和代币有什么本质区别？

加密货币是区块链中的原生资产，如BTC

代币是区块链中智能合约产生的资产。

（2）在该应用场景中，使用哪种更合适？请说明理由。

用代币。理由它可以随意控制发行量、通货膨胀、进行增销/销毁，维持经济运行。

2、某画家在区块链上售卖具有唯一性和收藏价值的数字画作；其朋友开发区块链游戏，需管理大量完全等价的游戏金币。

（1）请解释什么是同质化代币和非同质化代币，并分别写出它们的以太坊标准名称。

同质化代币：每个代币的价值和属性相同，可互换与分割，ERC-20

非同质化代币：每个代币价值和属性独一无二，不可分割与互换，ERC-721

（2）上述两个应用场景中，应分别使用哪种代币类型？为什么？

画家用非同质化代币，收藏品具有唯一和珍贵性。

游戏金币用同质化代币，可随意发布数量和控制通货膨胀。

3、请简要描述ERC20标准中的单步转账和两步式转账各自的流程。

单步转账，由A直接调用transfer函数，把资金转入B账户。

两步式转账（approve+transferFrom），授权第三方进行代币转账

4、简述私有链、联盟链和公有链，并举出各自一个应用场景和一个典型共识算法。

私有链：私人直接所有，权限集中；企业内部审计；Raft

联盟链：半中心化，参与需许可；供应链金融；拜占庭容错；

公有链：完全去中心化，任何人可参与；加密货币；工作量证明

5、为什么“女巫攻击”是公有链必须防范的攻击手段？并举一种防范女巫攻击的共识机制。

公有链任何节点可参与，攻击者可制造大量虚拟节点造成不成比例的影响力，从而破坏共识。

工作量证明与权益证明

6、请简要说明为什么联盟链不易受到女巫攻击。

联盟链加入是审核机制。每个节点的身份在真实世界中都经过审核与校验。

1、简述区块链链上扩容和链下扩容区别。

链上扩容：直接在区块链主链上的进行协议修改

链下扩容：把大量交易转移到主链之外的第二层网络，最终结果在主链上结算

2、状态通道（或闪电网络）原理。

双方锁定一笔资金，共同开启“交易通道“，可进行无限次交易，交易与签名不上链，在最后结果结算在主链上进行，提升效率和降低交易费。

3、隔离见证扩容原理。

将数字签名数据与主要的交易数据分离开

4、如何理解隔离见证是软分叉。

具备向后兼容。旧节点能接受新区块为有效，只是不理解内部数据结构。