2023年上海市高等学校信息技术水平考试试卷

二三级 区块链技术及应用（模拟卷）

（本试卷考试时间 150 分钟）

一、单选题（ 本大题 15 道小题 ，每小题 3 分，共 45 分），从下面题目给出的A、B、C、D四个可供选择的答案中选择一个正确答案。

1. 区块链的发展阶段不包括_____。

A.可编程货币
B.可编程合约
C.可编程金融
D.可编程社会

2. 去中心化系统的特点为_____。

A.无绝对权威节点
B.树状结构
C.由少数节点维护规则
D.效率高

3. Base58去掉了Base64编码中容易引起混淆和转义的字符，这些符号在打印、阅读、互联网上进行转发时可能造成歧义。Base58不包含_____。

A.0（数字0）
B.1（数字1）
C.o（小写字母o）
D.i（小写字母i）

4. 对HASH函数的特点描述错误的为_____。

A.输入长度任意
B.固定映射
C.输出位数固定
D.可逆

5. 区块链链式数据结构依赖于_____。

A.哈希函数
B.椭圆曲线
C.共识机制
D.区块时间戳

6. 51%攻击的特点是_____。

A.黑客的常用攻击手段
B.可以利用共识机制解决
C.利用更长链进行篡改
D.利用假节点进行攻击

7. 非对称密钥体制的描述中，不正确的是_____。

A.发送方利用接收方公钥加密
B.发送方利用接收方私钥加密
C.接收方利用发送方公钥验证签名
D.发送方利用自己私钥进行签名

8.比特币区块体中未包含_____
A.手续费
B.挖矿奖励(coinbase)交易
C.交易信息
D.默克尔树根

9. 区块链中常见的工作量证明共识为_____。

A.POW
B.零知识证明
C.DPOS
D.PBFT

10.Hyperledger Fabric 智能合约通常运行于_____。
A.EVM 环境
B.BVM 环境
C.容器环境
D.eWASM 环境

11. 以下的代码，说法错误的是:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.4.22;

contract fibonacci {
    uint [] fibseries;
    function generateFib(uint n) public {
        fibseries.push(1);
        fibseries.push(1);
        for (uint i=2; i < n ; i++) {
            fibseries.push(fibseries[i-1] + fibseries[i-2]);
        }
```

```
    }
}
```

A.程序是一个完整的智能合约
B.程序无法通过编译
C.程序可以正常运行
D.特定的输入可能导致 Gas 耗尽引起中断

12. 关于以下的代码，说法正确的是:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.3;
contract SimpleStorage {
    uint public num;

    function set(uint _num) public {
        num = _num;
    }

    function get() public view returns (uint) {
        return num;
    }
}
```

A.程序存在语法错误
B.程序不存在语法错误，但无法通过编译
C.程序可以通过编译，但无法初始化
D.程序可以运行

13. 关于比特币出块奖励的说法不正确的是_____。

A.出块奖励和区块中交易数有关
B.出块奖励和难度无关
C.出块奖励最终会减少为 0
D.出块奖励经过一段周期会减半

14.区块链共识不能解决_____。
A.51%攻击
B.伪造数据
C.记账权归属
D.规则升级

15. 阅读Solidity编写的智能合约代码，正确的说法是_____。

```
pragma solidity ^0.4.24;
```

```
contract CalcContract {
  uint memoryData;
  function add(uint a) public returns (uint result) {
      memoryData = a;
      return a+63;
  }
}
```

A.编译器版本大于 0.4.24
B.编译器版本小于 0.4.24
C.智能合约的名称是 CalcContract
D.智能合约的名称是 add

二、填空题（ 本大题 5 道小题 ，每空 3 分，共 30 分）。

1.在比特币区块交易将利用默克尔树的方式进行验证，在轻客户端向全节点请求验证一笔交易时，该全节点不仅需要提供该笔交易的内容，还需要提供相应证明，在此过程中除该笔交易本身的哈希值和默克尔树根外。一个区块有 256 笔交易时，至少需要返回_____个哈希值；有 120 笔交易时，至少需要返回_____个哈希值。

2.PBFT 共识中，100 个节点能容忍的最多不诚实节点数量为_____；POW 共识中，100 个节点能容忍的最多不诚实节点数量为_____。

3. 已知某个以太坊交易的Gas Price为0.000000021Ether，允许支付的最大手续费为0.00252Ether，则Gas Limit为____，已知合约中执行一次transaction操作的Gas消耗为$G_{transaction}$=21000，则该智能合约中最多可以成功执行____次transaction操作。

4.以太坊系统的_____数据通常是用 KV 键值对数据结构存储的，其中 K（键）的含义为_____。

5.比特币计算某个地址账户余额时，是通过遍历账户所有的_____并求和得出的；以太坊计算某个地址账户余额时，是通过读取账户的_____字段得出的。

三、操作题

（本大题2道小题，第一小题10分，第二小题20分，共30分）

1、【Solidity合约改错题】

说明：本合约程序代码中有三处错误，请分析源代码(C:\素材\p1.pdf)，找出错误行并修正错误。

注意：
将错误代码行号和正确代码保存在"C:\KS\p1答案.txt"中,仅在横线之间填入所编写的若干语句；语句可能为多行时请自行换行，请勿改动其余部分。

2、【Solidity合约填空题】

说明：本合约程序代码中有四处内容缺失，包括行号（8，12，33，49），请分析源代码(C:\素材\p2.pdf)，根据缺失部分的注释要求补全代码内容。

注意：

将缺失部分代码保存在"C:\KS\p2答案.txt"中，仅在横线之间填入所编写的若干语句；语句可能为多行时请自行换行，请勿改动其余部分。

四、综合分析题

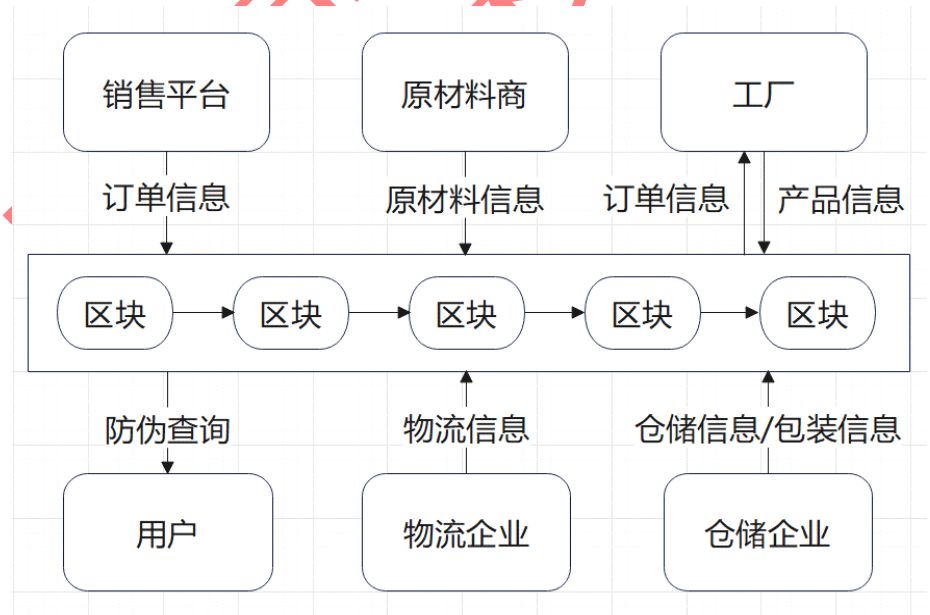
（本大题2道小题，第一小题15分，第二小题30分，共45分）

1、【场景分析】

请针对指定的场景进行分析，完成所需的步骤。

一个工厂采用用户下单才生产的模式，使用区块链追溯产品。用户通过销售平台下单，销售平台记录订单信息；工厂收到订单信息后，向原材料商采购原材料，原材料商记录原材料信息；工厂完成产品生产后记录信息，发送至仓储企业进行仓储；仓储企业包装产品并记录信息，随后交付给物流企业进行运输；物流企业记录物流信息；用户接收到产品后即可在区块链上查询中间过程产生的信息，确保产品来源可靠。

如图所示：



步骤一：设计组织间合作方式，选择合适的链架构，并说明理由。

步骤二：请分析参与场景的角色，分析设计身份管理模式（公私钥/证书等），并说明理由。

步骤三：请分析场景中出现的数据，选择合适的数据存储模式，讨论隐私保护需求。

注意：

将填空内容保存在"C:\KS\p3答案.txt"中，仅在横线之间填入答案内容，请勿改动文档的其他部分。

2、【场景分析】

场景说明：Hyperledger Fabric可以用来搭建联盟链，某国家现为了解决大型赛事中的数据传输问题组建一个联盟，其中有5个组织：体育场馆（org1）、医疗机构（org2）、铁路机构（org3）、航空机构（org4）和政府机构（org5）。该联盟决定利用区块链合作传输数据，包括公共数据和隐私数据1（防疫信息）、隐私数据2（旅行信息）。

需求：

1.联盟商定每个组织创建2个节点，除此以外，政府机构额外承担排序节点工作，每个排序节点只服务一个通道。

2.公共数据可由所有机构访问；隐私数据1（防疫信息）只能由医疗机构和政府机构访问；隐私数据2（旅行信息）只能由铁路机构、航空机构和政府机构访问；各类数据之间需要隔离。

3.处理公共数据的智能合约有CCPublic1和CCPublic2；处理隐私数据的智能合约有CCPrivate1（防疫信息）和CCPrivate2（旅行信息）。

4.请完成项目的区块链架构设计。

注意：

(1)请关注架构设计，除要求填空的位置之外，请勿改动文档的其他部分。

(2)将填空内容保存在"C:\KS\p4答案.txt"中,仅在横线之间填入所编写的若干语句；语句可能为多行时请自行换行，请勿改动其余部分。