**2020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（A 场）**

（本试卷考试时间 150 分钟）

**一、单选题 ( 本大题 25 道小题 ，每小题 3 分，共 75 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.大多数区块链的网络技术基于（ ）。

A.HTTP

B.P2P

C.FTP

D.POP3

2.比特币是区块链（ ）的代表。

A.1.0

B.1.1

C.2.0

D.3.0

3.（ ）是比特币区块链的特点。

A.链路加密

B.中心化

C.数据不可篡改

D.不公开

4.某公司要将人力资源系统改造成“区块链+”，且不和其他公司/机构共享数据，则该区块链应选用（ ）。

A.公有链

B.私有链

C.产业链

D.联盟链

5.（ ）不属于区块链共识层。

A.激励机制

B.PBFT

C.P2P

D.PoS

6.以下（ ）不是哈希函数。

A.SHA256

B.SHA1

C.Base256

D.MD5

7.（ ）使用DPoS共识机制。

A.比特币

B.以太坊

C.EOS

D.莱特币

8. Secp256k1使用了y2= x3+a mod p曲线，其中a=（ ）。

A.3

B.5

C.7

D.11

9.Hyperledger Fabric中使用（ ）实现交易的背书。

A.PoW

B.对称加密

C.数字签名

D.共识机制

10.当有n笔交易，那么利用默克尔树验证交易隶属关系的时间复杂度是（ ）。

A.O(log n)

B.O((log n)^2)

C.O(n)

D.O(n^2)

11.在Hyperledger Fabric中，CA节点的功能是（ ）。

A.接收交易，对未打包的交易进行排序生成区块并广播

B.接收客户端的注册申请，返回注册密码用于用户登录，以便获取身份证书

C.负责验证从排序服务节点发送的区块里的交易，维护状态数据和账本的副本

D.执行交易并对交易结果进行数字签名

12.下列说法中，（ ）不是共识机制PoW和PBFT的区别。

A.PoW算法需要矿工消耗算力计算密码学难题，而PBFT不需要

B.采用PoW的区块链可能会产生分叉，采用PBFT的区块链不会产生分叉

C.采用PoW时可以容忍49%作恶节点，采用PBFT时可以容忍(n-1)/3个作恶节点

D.PoW支持的节点数量较少，而PBFT可支持的节点数量较多

13.以太坊的每笔交易都会收取一定数量的（ ）作为手续费。

A.BTC（比特币）

B.Oil

C.Gas

D.XRP（瑞波币）

14.在比特币中使用了Base58的改进版本（ ）。

A.Base58Check

B.Base58Update

C.Base64

D.Base128

15.Hyperledger Fabric 提供（ ），实现了灵活的企业账户管理。

A.P2P网络

B.通道（channel）

C.MSP

D.微服务机制

16.在以太坊平台上创建的数字货币一般遵循（ ）。

A.RSA 标准

B.ERC-20 标准

C.Secp256k1 标准

D.ECDSA 标准

17.区块链不能抵御（ ）。

A.消息重放攻击

B.双花攻击

C.51%攻击

D.女巫攻击

18.（ ）技术可以确认区块链中交易的正确性和交易的发起方。

A.数字签名

B.共识算法

C.哈希算法

D.奖励机制

19.分布式账本系统架构从整体上可划分为数据层、网络层、共识层、智能合约层和（ ）。

A.表现层

B.应用层

C.密码层

D.物理层

20.TheDAO 项目导致大量数字货币被盗的原因是（ ）。

A.智能合约漏洞

B.女巫攻击

C.51%攻击

D.双花攻击

21.比特币区块间维持链式结构的方式（ ）。

A.时间戳

B.默克尔树

C.区块高度

D.哈希指针

22.根据（ ），以太坊交易可分为消息执行和转账交易。

A.交易发送者地址类型

B.交易接收者地址类型

C.是否有Gas Limit

D.是否有data字段

23.用比特币交易的第一个商品是（ ）。

A.汉堡

B.意大利面

C.三明治

D.披萨

24.Hyperledger Fabric利用（ ）运行智能合约。

A.Java VM

B.EVM

C.FPGA

D.容器

25.关于比特币挖矿奖励的说法正确的是（）。

A.参与挖矿就有奖励

B.挖矿奖励的比特币数量是不变的

C.最初的挖矿奖励是50枚比特币

D.挖矿奖励过一年减半

**二、操作题**

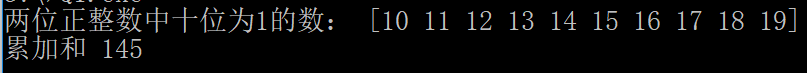
**素材、样张、KS目录均在zip文件中，可双击此图标打开**

**2.1 GO语言编程**

**程序功能说明：**将两位正整数中十位为1的数依次放入数组a中，打印输出数组a及数组内所有元素之和。

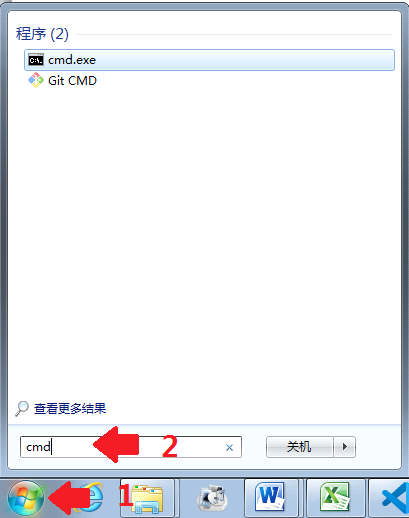
**程序源代码在“C:\素材\p1.go”中，请根据源代码和功能说明完成程序缺失部分，将所写代码保存在“C:\KS\p1答案.docx”中。要求程序输出结果与题目要求一致。**

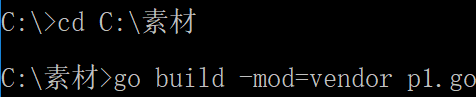
**程序结果应输出如下：**



如需编译，请点击开始菜单，输入cmd，调出命令行界面，切换至“C:\素材”目录下，使用go build -mod=vendor p1.go指令。

如下图所示：





**2.2 GO语言智能合约编程**

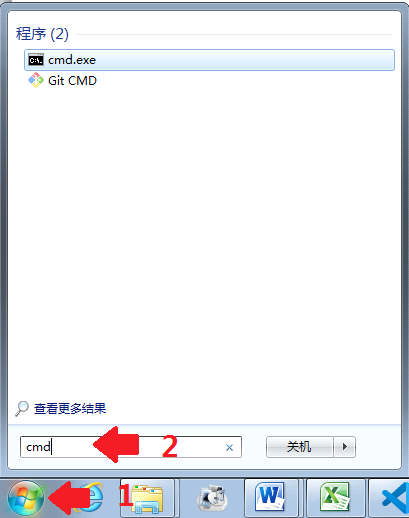
**功能说明**：使用GO语言实现超级账本智能合约**FoodContract**。

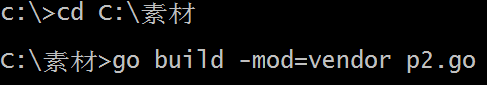
**请根据源代码“C:\素材\p2.go”的注释和功能说明完成程序缺失部分，将所写代码保存在“C:\KS\p2答案.docx”中。**

**提示：**智能合约API参见“**C:\素材\API.docx”**。

如需编译，请点击开始菜单，输入cmd，调出命令行界面，切换至“C:\素材”目录下，使用***go build -mod=vendor p2.go***指令。

如下图所示：





**2.3 综合题**

**请阅读如下材料，完成项目的区块链架构设计，在“C:\KS\p3答案.docx”文件中填写完成所需步骤。**

Hyperledger Fabric可以用来搭建联盟链，现有一个名为university.cn的联盟，其中有5个组织org1、org2、org3、org4和org5决定利用区块链合作传输数据，包括公共数据和秘密数据。联盟商定每个组织创建2个节点，org5额外承担排序节点工作，公共数据允许全部组织访问，秘密数据只允许org1、org3和org5访问。处理公共数据的智能合约有CCP1和CCP2；处理秘密数据的智能合约有CCS1和CCS2。