2024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 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._____不是区块链的数据组织特色。

A.利用哈希函数计算数据块特征，并利用特征进行关联的链块式结构

B.利用数字签名保护交易数据

C.利用易于验证的树状结构防止数据被篡改

D.使用集中式服务器管理和控制数据

2.根据参与组织的不同特点，可将区块链分为三类。不属于该分类的是_____。

A.私有链

B.联盟链

C.许可链

D.公有链

3.比特币所使用的数字签名算法是_____。

A.DES

B.RSA

C.SHA256

D.ECDSA

4._____是指由多个节点协同完成，并在每个节点完整记录下来的交易日志。

A.共识机制

B.分布式账本

C.智能合约

D.数字签名

5.在比特币中，大多数需要向用户展示的数据都使用Base58Check编码，下面不属于其作用的是_____。

A.实现数据加密

B.避免字符混淆

C.使用版本前缀标识数据的类型

D.实现错误校验机制，增强了传输数据的安全性

6.对于以太坊中的外部账户，其记录的字段中_____项为空。

A.nonce值

B.余额

C.存储
D.合约代码哈希

7.以太坊最初使用_____共识协议。

A.PoW (Proof of Work)
B.PoS (Proof of Stake)
C.DPoS (Delegated Proof of Stake)
D.PBFT (Practical Byzantine Fault Tolerance)

8.PoS（权益证明）共识机制中，出块的概率与_____相关。
A.节点的网络带宽
B.节点拥有的数字货币数量
C.节点的 CPU 性能
D.节点的内存大小

9.作为第二代区块链系统，以太坊提供一个非常重要的功能_____。

A.准入门槛
B.智能合约
C.匿名信息
D.点对点支付

10.在基于链式结构的分布式账本系统中，如果同时收到两份合法的账本，应_____。

A.保留本次挖矿手续费最高的交易分支作为主账本
B.保留交易时间最早的分支作为主账本，但是保留其它分支
C.保留交易时间最新的分支作为主账本
D.保留当前最长分支作为主账本

11.区块链智能合约的自动执行是由_____驱动的。

A.用户的指令
B.中央服务器的控制
C.共识机制的规则
D.合约管理者的授权

12. 如下代码定义了ERC20代币合约接口，说法正确的是_____。

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

interface IERC20 {
    event Transfer(address indexed from, address indexed to, uint256
value);
```

```
    event Approval(address indexed owner, address indexed spender,
uint256 value);
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address to, uint256 amount) external returns
(bool);
    function allowance(address owner, address spender) external view
returns (uint256);
    function approve(address spender, uint256 amount) external returns
(bool);
    function transferFrom(address from, address to, uint256 amount)
external returns (bool);
    function name() external view returns (string memory);
    function symbol() external view returns (string memory);
    function decimals() external view returns (uint8);
}
```

A. 实现该接口的合约代码只能包含 2 个事件
B. 实现该接口的合约代码不能包含更多变量
C. 实现该接口的合约代码可以包含更多的事件和函数
D. 实现该接口的合约代码可以省略某些事件和函数

13. 关于以下代码，说法正确的是_____。

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.3;
contract c1 {
    uint public i = 0;
    function kill() public {
        while (true) {
            i += 1;
        }
    }
}
```

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

14. 关于以下代码，说法正确的是_____。

```
function add(uint256 a, uint256 b) public returns (uint256) {
    uint256 c = a + b;
    return c;
}
```

A.代码存在语法错误
B.代码不存在语法错误，但无法通过编译
C.代码运行结果可能 c<a
D.代码运行结果 c>=a

15. 关于以下代码，说法正确的是_____。

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.3;
contract c1 {
    uint public x = 1;
    function addToX(uint y) public pure returns (uint) {
        return x + y;
    }
}
```

A.代码存在语法错误
B.addToX 函数只能在当前合约内访问
C.代码尝试修改了状态变量（State）
D.代码尝试修改了本地变量（Local）

二、填空题（ 本大题 5 道小题 ，每空 3 分，共 30 分）。

1.已知某区块链节点算力相同，且最多包含 19 个不诚实节点，则在采用 PoW 共识协议的情况下，该区块链的节点总数不低于_____个；在采用 PBFT 共识协议的情况下，节点总数不低于_____个。

2.某区块包含 64 笔交易，在已知交易哈希时，则需要经过_____次哈希计算，才能构建一棵默克尔树。若轻节点需要证明某笔交易是否存在于该默克尔树中，除该笔交易本身的哈希值和默克尔树根外，需要向全节点请求_____个哈希值。

3. 在以太坊中，某个交易的Gas Price是0.000015Ether，允许支付的最大手续费为3.1Ether，已知合约中执行一次transaction操作的Gas消耗为$G_{transaction}$=21000，执行一次newaccount操作的Gas消耗为$G_{newaccount}$=25000，已知该交易执行了4次newaccount操作，还能够最多执行_____次transaction操作，执行完后还剩下_____Ether手续费。

4.如果用户 A 拥有一个 5 比特币的 UTXO 和一个 2 比特币的 UTXO，A 想买用户 B 的一个 6 比特币的物品，此时这笔交易的输入就是 7 个比特币的 2 个 UTXO，当不考虑手续费时，输出时返回一个给 A 账户的_____比特币的 UTXO 和一个给 B 账户的_____比特币的 UTXO。

5.PBFT 算法的核心是三阶段共识流程，分别为_____、_____、提交阶段。

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】

本合约是为了宠物购买的DAPP所准备的，具体要求参见注释，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：

将错误代码行号和错误原因保存在"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】

本合约程序代码中有四处内容缺失（行号55，105，118-120，141），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，依赖的源文件在C:\素材\依赖的sol合约\。

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。

通过区块链记录学习经历，可以构建学生的终身学习档案，以下是一个实际的应用场景：

学校或培训机构记录学生学习经历，包括学习内容、考试成绩等；

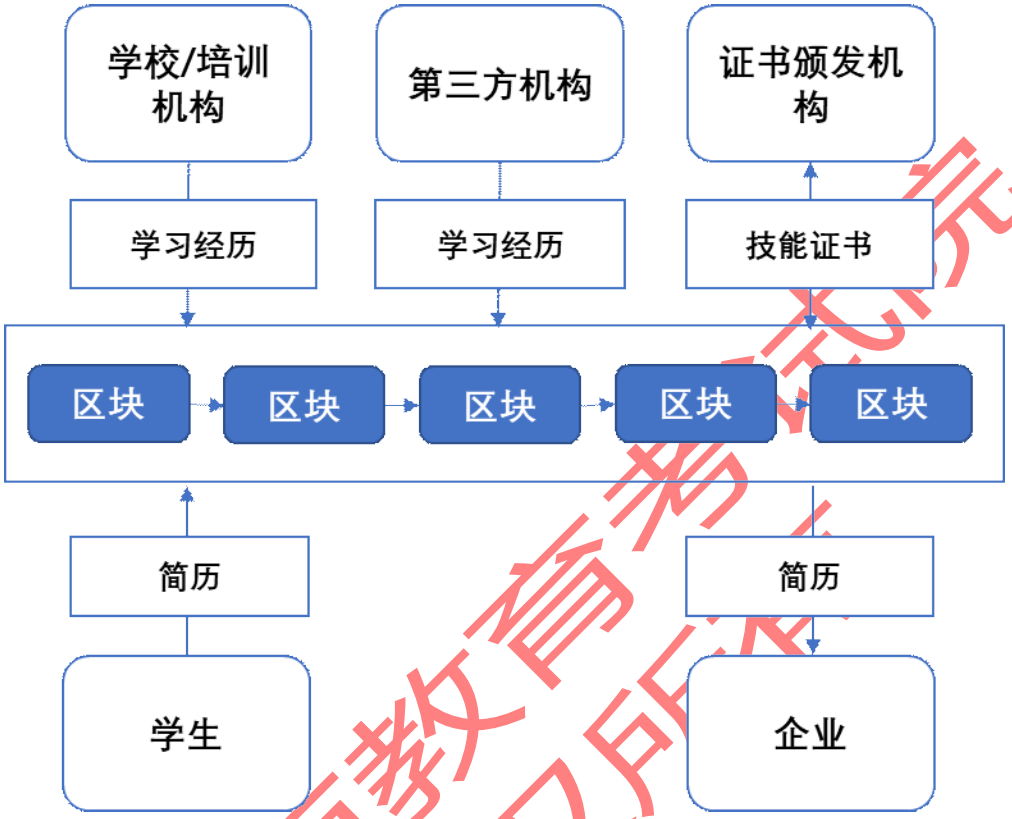
第三方机构记录学生竞赛、公益活动等经历；

证书颁发机构通过学习经历发放对应的资格证书；

学生生成简历，内容由区块链背书，投递给指定的企业；

企业收取简历，通过区块链验证真实性，简化背调流程；

如图所示：



步骤一：请设计组织、用户间合作方式，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、【区块链架构设计】

请阅读如下材料，完成项目的区块链架构设计，在答题纸中填写完成所需步骤。（题目描述场景为模拟场景，并不准确对应现实场景）

为了解决企业生产资金问题，多个机构组建联盟展开合作，当前有7个机构加入联盟：企业1（ent1），企业2（ent2），企业3（ent3），税务机构（tax1），银行1（bank1），银行2（bank2），政府数据中心（data1）。

现在制订如下规则：

1. 企业记录经营情况记录，记录企业间往来信息；
2. 企业间往来信息需要经过往来企业认可；
3. 税务机构记录企业纳税情况；
4. 银行在获得合理证明资料后，可以给企业提供贷款；
5. 企业在申请贷款时，授权必要数据给银行，其他机构不可以访问相关数据；
6. 银行获取经营情况记录（企业自身背书），往来信息（多方背书），纳税情况（税务机构背书），判断合理性，为企业提供贷款；

根据已知信息，数据包括：

1. 经营情况记录，由企业记录；
2. 企业间往来信息，由参与企业确认有效性；
3. 企业纳税情况，由税务机构记录。

本联盟区块链基于Hyperledger Fabric构建，每个有**记录权限**的组织各创建2个节点，由政府数据中心承担排序节点工作。

所有机构仅可访问自己记录的数据以及被授权访问的数据。

系统中已设计如下的智能合约，若不能满足题目要求，请自行增加并说明：

1. 处理经营情况记录的 CCEntRecord；
2. 处理企业纳税情况的 CCTax。

注意：

(1)请注意题目要求，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，仅在横线之间填入答案内容。