**特许全球金融科技师（CGFT）一级**

**《区块链技术原理及应用》考试大纲**

（修订日期： 2022年10月25日）

[一、 考试性质 2](#_Toc114677934)

[二、 考查目标 2](#_Toc114677935)

[三、 考试形式和试卷结构 3](#_Toc114677936)

[1. 试卷满分 3](#_Toc114677937)

[2. 答题方式 3](#_Toc114677938)

[3. 试卷内容结构 3](#_Toc114677939)

[4. 试卷题型结构 3](#_Toc114677940)

[四、 考察内容与考点解析 4](#_Toc114677941)

[1. 章节内容考点清单 4](#_Toc114677942)

[2. 重要高频考点题目 19](#_Toc114677943)

[五、 历年真题与考试样题 20](#_Toc114677944)

# 考试性质

特许全球金融科技师（CGFT）一级包含《区块链技术原理及应用》科目，区块链技术是金融科技基础技术，特许全球金融科技师（CGFT）一级考试是认证性考试，按照金融科技人才知识技能能力标准，以标准化考试的方式对考生对于区块链技术原理及应用知识的掌握程度进行评价。

# 考查目标

1. **知识技能要求**

CGFT一级对考生区块链技术原理及应用相关知识要求如下：

* 理解区块链技术的基本概念，包括区块链核心功能，如基础账本、共识机制、智能合约、挖矿、激励机制。区块链业务功能，如去中心化组织、隐私保护、区块链的安全、运维和治理等。
* 了解区块链技术的技术原理，如密码学、分布式系统、点对点网络，跨链技术以及区块链的性能优化等。
* 了解区块链技术的场景应用，包括在币圈和链圈的应用，如虚拟货币、钱包、稳定币、法定数字货币、智能合约、数字资产交易、供应链金融等。
* 了解区块链产业的发展趋势和投资前景，并能甄别对区块链技术和应用认识误区。

1. **能力素质要求**

CGFT一级对考生区块链技术原理及应用相关能力素质要求如下：

* 在理解区块链技术原理的基本概念、技术原理和场景应用基础上，能够在实际业务场景中灵活应用相关技术，并能在技术应用解决方案构建方面有一定的创新。
* 对区块链技术的发展趋势有较相对准确客观的分析判断能力。

# 考试形式和试卷结构

## 试卷满分

CGFT一级考试包含七门课程，其中《区块链技术原理及应用》包含40题，该部分满分为100分。

## 答题方式

机考，闭卷，可以跨区答题

## 试卷内容结构

不对内容结构分布做明确限定。

## 试卷题型结构

以客观题方式进行考察，题型包括：判断题、单选题、多选题。

不对题型结构分布做明确限定。

# 考察内容与考点解析

## 章节内容考点清单

本表中考察要求的定义如下

* 基础识记：主要是事实知识，考察对事实性知识的记忆，“知道”即可。
* 一般理解：主要是概念定义，仅需一般理解。
* 深入理解：主要是核心原理，需要较深入理解并能灵活应用。
* 不做要求：不作为考试内容，考生可以自主选择阅读。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 章 | 节 | 考点 | 考查要求 | 重要性 | 难度 |
| 1. 导言 | 1.1信任架构的演化 | * 信任架构演进：“中介”的发展与异化 * 数字化进程及数字孪生 * 信任架构变革：建立在数学、算法基础 上的信任 | 基础识记 | 高 | 低 |
| 1.2 “区块链”何以得名 | * “blockchain”译名，2014 年以前区块链技术以“比特币”统通而称之 * 2014-2015 以太坊问世 | 基础识记 | 低 | 低 |
| 1.3“距离坍缩”与信任路径再定义 | * 区块链改变生产关系 * 区块链缩短“信任距离” * 区块链导致“信任距离坍缩” * 区块链自带“治理理念”、“商业模式” | 基础识记 | 低 | 低 |
| 1. 密码学基础（1） | 2.1 密码学的定义 | * 密码学定义：研究仅在受限范围内共享信息的机制的科学 * 密码学基本场景--隐秘通信：信息发送方、信息接收方、信道、截听者。 | 基础识记 | 高 | 低 |
| 2.2 密码学的历史 | * 新观念的核心是：密码变换的算法可以是公开的，运行算法所依赖的一段信息的内容是秘密的，这段秘密的信息被称为“密钥” * 加密体制分为：对称加密和非对称加密。 | 基础识记 | 高 | 低 |
| 2.3 对称加密 | * 对称加密是加密变换和解密变换采用同一个密钥的密码体制。 * 重要手段：乱序和扩散。 * 对称加密优点：1. 速度快。2. 简单。3. 相对安全。 * 对称加密缺点：1.分发困难。2.两两复杂性。 | 基础识记 | 低 | 低 |
| 2.4 哈希（散列） | * 哈希函数特性：1. 单向性。2. 防碰撞性。3.压缩性。4.抗差分攻击性 * 哈希（散列）函数的作用： 存证、浓缩、签名 | 基础识记 | 高 | 低 |
| 1. 密码学基础（2） | 3.1 非对称加密 | * 所谓非对称加密是指为隐私信息共享的每个参与方配置一对密钥，分别称为公钥和私钥 * 非对称加密的过程是非对称加密机制的“正向使用”，指的是发送方用对方的公钥加密，接收方用自己的私钥解密 | 一般理解 | 高 | 低 |
| * 1. 数字签名及检验 | * 数字签名的过程，是非对称加密机制的“反向使用”，发送方用自己的私钥加密，接收方用对方的公钥解密。 | 一般理解 | 低 | 低 |
| 3.3 非对称加密体制的数学原理 | * 非对称加密体制RSA，大数分解在数学上的固有难度 * 一旦能够运行Shor算法的量子计算机突破，RSA算法就不再安全。 | 一般理解 | 高 | 中 |
| 3.4公钥证书体系 | * 公钥和身份绑定问题，互联网应用中设立证书颁发中心，用公钥签名为公钥和身份绑定来背书。 * 区块链公链中，并不追求身份信息的公开透明，故不倾向使用CA/PKI数字证书体系。 | 一般理解 | 低 | 中 |
| 1. 分布式系统与点对点网络 | 4.1分布式系统简介 | * 分布式系统要由若干台通过网络连接在一起的计算机，其中每台计算机称为一个节点。 * 每个节点上涉及全局工作状态的记录称为一个“副本”，把为系统提供准确的全局工作状态称为“服务”。 * 对各个“副本”的关键性诉求：1. 一致性诉求。2.可用性诉求。3.分区容忍性诉求。 | 基础识记 | 高 | 低 |
| 4.2 CAP原则 | * CAP原则告诉我们，一致性诉求、可用性诉求、分区容忍性诉求，这三个需求不可兼得。 * 在区块链技术中，拜占庭容错是共识机制的核心诉求。 | 基础识记 | 低 | 低 |
| 4.3拜占庭将军问题 | * “拜占庭容错”指的是即使在分布式系统中有恶意节点存在的情况下，整个系统仍能按照预期提供正确的服务。 * “拜占庭容错”假设：（1）最终同步 （2）合理多数 | 基础识记 | 高 | 低 |
| 4.4点对点网络简介 | * 节点之间靠连接的接力可以把需要更新的全局状态传遍每一个节点，由此形成的网络称为点对点网络。 * 分布式是一种技术架构，去中心化是一种治理模式，去中心化以分布式为技术基础，但分布式并不必然导致去中心化。 | 基础识记 | 低 | 低 |
| 1. 区块链的诞生与发展知识点 | 5.1 比特币之前的探索 | * 早期探索共同弱点：没有摆脱对于可信第三方的依赖 | 基础识记 | 高 | 低 |
| 5.2 比特币与区块链1.0 | * 2008年10月31日，作者 Nakamoto Satoshi (中本聪）在密码学网站metzdowd.com发表比特币白皮书 * 比特币技术基础：密码学、分布式系统、点对点网络 * 比特币作为集成技术体系，实现协议创新、集成创新和商业模式创新 * 协议创新：实现了时间不可逆的数据组织方式 -- “区块链”; 完整提出并论证了“工作量证明”共识机制；初步解决了“双花”问题；提出了实现在不守恒的信息网络上传输守恒的价值的协议框架。 * 集成创新：集成了密码学、分布式系统、对等网络 * 商业模式创新：自带发行、自带激励的社区化公链运作模式 | 基础识记 | 高 | 低 |
| 5.3区块链进入2.0时代 | * 2.0时代标志性事件：俄罗斯天才少年”V神“, Vitalik Buterin, 推出”以太坊“。 * 在基础账本之上引入智能合约和虚拟机扩充区块链功能，引入 GAS 用经济手段解决调控计算资源的难题。 * 链圈的诞生 -- 面向区块链技术开发及应用的联盟化组织：超级账本(Hyperledger) 和 R3 | 基础识记 | 低 | 低 |
| 5.4 区块链的分类与业态 | * 区块链分类：公链、私链、联盟链 * 私链和联盟链也称为“许可链” * 联盟链业态：一强多弱型、多强型、多弱型 | 基础识记 | 低 | 低 |
| 5.5 区块链3.0在召唤 | * 区块链3.0、数字货币 | 不做要求 | 低 | 低 |
| 1. 基础账本 （1） | 6.1 时间不可逆性 | * 区块链的“不可篡改（撤销）、不可仿冒、不可抵赖、不可乱序”特性为区块链的基础技术服务 * 区块链的用户之间可以不存在信任基础，但只要他们都信任数学和算法，就可以基于区块链建立信任。所以说，区块链是在非信任环境下提供信任服务的基础设施 * 区块链在业务层面提供不可透支、不可双花的价值转移服务。 * 人们还在努力把隐私保护和可运维性等治理功能也实现在区块链上 | 基础识记 | 高 | 低 |
| 6.2 集中与分布式记账 | * 区块链的“存证+定序”功能提供了坚实的密码学基础 * 大部分分布式系统是区块链但也有少部分不是区块链；区块链不都是分布式账本 | 一般理解 | 高 | 低 |
| 6.3 存证结构 | * 区块链通过建立数据区块之间基于哈希函数的勾稽关系，在信息世界中实现了时间的不可逆性 * 区块链的存证结构依赖的是“上一区块的哈希值”、“本区块的哈希树根”、“本区块的随机配数”这三个特征数与“本区块的哈希值”之间的验算关系。 | 深入理解 | 高 | 高 |
| 6.4 工作量证明 | * 存证和定序能够获得多高程度的安全保障，取决于我们投入多大的工作量来重新组织数据，花多大的代价让数据上链 | 基础识记 | 低 | 低 |
| 1. 基础账本 （2） | 7.1 价值守恒 | * 区块链上价值流通的两个模型：被比特币所采纳的 UTXO模型和被以太坊所采纳的账户 - 余额模型。 * 就构建“价值互联网”这一愿景而言，价值与信息最根本的不同是信息可以是不守恒的，价值必须是守恒的 * 传统金融机构实现价值转移的方式是不可自证的 * 区块链的基础账本中，实现了可自证的满足守恒性的价值转移。因为区块链除了区块之间的哈希勾稽关系之外，还包括了在价值转移过程中必须满足的守恒性约束。 | 深入理解 | 高 | 高 |
| 7.2 价值流通的UTXO模型 | * UTXO代表Unspent Transaction Output（未花费的交易输出） * UTXO的特点：1.可自证真实的转账记录，是一笔转账交易的真实凭据。2. 是一个尚未花费的转账记录。3.是一个支配权有明确归属的转账记录。 | 基础识记 | 高 | 低 |
| 7.3价值流通的账户 - 余额模型 | * 账户 - 余额模型对每一个账户可支配的每一种资产类型，均设置了一个余额状态 | 基础识记 | 高 | 低 |
| 7.4价值流通的基本约束条件 | * 等式约束： 转出价值 + 剩余价值 = 原有价值 * 不等式约束： 原有价值 >= 转出价值 * 守恒约束： 一方的转出价值必须等于对手方的转入价值 | 一般理解 | 中 | 低 |
| 7.5区块链基础账本的安全性 | * 基础账本的数据可靠性，通过区块链特有的存证+定序功能完成 | 一般理解 | 中 | 低 |
| 1. 共识机制 (1) | 8.1共识机制的定义、意义和分类 | * 在区块链中，依靠群体参与见证，用事先确定的规则对见证的结果进行综合，最终达成被所有参与者认可的共识结论的机制，称为共识机制。 * 在共识形成过程中，一些节点可能故意见证错误的内容, 一些正确的内容受网络状况的影响可能很晚才被见证, 一些诚实节点可能先见证了错误的内容，之后才更改为正确的内容 * 共识机制可分为：基于证明的、基于投票的 和 基于随机性的。 * 基于证明的共识机制：POW(工作量证明)、POS(权益证明) 和 DPOS (受托权益证明) * 基于投票的共识机制：PBFT （实用拜占庭容错） * 基于随机性的共识机制: AlgoRand | 深入理解 | 高 | 中 |
| 8.2 POW | * 假设多数人诚实记账 * 随着时间推移，诚实记账者看到的终究会传播到所有诚实记账者那里 * 对POW共识机制有效攻击方式“51%”算力攻击 | 一般理解 | 中 | 低 |
| 8.3 POS | * 账本上存储了更多价值的用户更倾向于诚实记账 * 把记账权“份额化”，不同的记账权份额对应不同的寻找随机数的难度 * 黑客可利用可操作份额攻击 | 一般理解 | 低 | 低 |
| 8.4 DPOS | * “超级节点”代替份额拥有者行使记账权 * 算力集中，风险也集中 | 一般理解 | 低 | 低 |
| 8.5 小结 | * POW : 效率低、安全高、开放 * POS: 效率中、安全中、开放 * DPOS: 效率高、安全低、开放 | 基础识记 | 中 | 低 |
| 1. 共识机制 (2) | 9.1 PBFT的场景设定 | * PBFT算法相关论文最初发表于1999年 * 预设场景和前提条件: 成员固定假设：所有节点一经加入就不能退出; 最终同步假设：所有“在途”的信息，经过一段固定时间的等待，最终会被收到; 坏人假设：每个节点都有成本“恶意”节点的可能; 透明性假设：节点之间传递的信息，其他节点都有办法“嗅探”到，但不能截断或篡改，也不能验证信息的完整性。 * 任务：服务的准确状态要复制到每个副本，每个副本都要对所经历的状态序列达成共识。 | 一般理解 | 高 | 中 |
| 9.2 PBFT的共识流程 | * PBFT消息状态的正常顺序 request、pre-prepare、prepare、commit、reply | 一般理解 | 高 | 中 |
| 9.3 PBFT的拜占庭容错能力和适用场景 | * PBFT共识机制特别适合于联盟链与私链 | 一般理解 | 高 | 中 |
| 9.4 共识机制的改进之路 | * 当见证者人数增加时，两两通信的复杂性大大增加，构成巨大的性能压力 * 共识机制改进优化的趋势：“从多到少、从链到图、从确定到随机” | 基础识记 | 中 | 低 |
| 1. 智能合约概论 | 10.1智能合约与可编程性 | * 智能合约是基于基础账本的，包含价值和信任状态为内容的程序代码，它可以在外部消息的作用下按照既定的业务逻辑实现价值的再分配。 * 智能合约离不开基础账本。 * 智能合约使区块链可以依据一定的内在逻辑和外界输入，实现价值的再分配。 * 一个区块链如果仅含基础账本，不能对外界变化做出实时反应；不能包含复杂的业务逻辑；不转账就不流动，不能充分发挥数字化世界的特点。 | 深入理解 | 高 | 中 |
| 10.2智能合约的要件 | * 智能合约要件：基础账本、编程语言、虚拟机 | 基础识记 | 高 | 低 |
| 10.3 如何用智能合约体现“业务逻辑” | * 智能合约可以表达从简单到复杂的各种业务逻辑，随着“业务逻辑”的更加复杂，合约对相关人行为的引导作用也更加精细 | 基础识记 | 低 | 低 |
| 10.4 智能合约的可信性 | * 智能合约的可信度可以分为：1. 外部信息源是否可信 2. 智能合约的运行结果是否可信 * 外部信息源可信度技术解决手段 “预言机” (Oracle), 预言机是经过“标准采集接口+特殊共识处理”的可信外部信息源 * 虚拟机可信度问题解决方法：对智能合约的执行状态和结果进行跟踪和留痕 | 一般理解 | 中 | 低 |
| 10.5 智能合约能否代替真正的合约 | * 智能合约的编程语言必须具有一定程度的人类可读性，这样可以使得智能合约的参与者提前判断合约代码的含义和其中的风险 | 基础识记 | 中 | 低 |
| 1. 智能合约的设计 | 11.1环保众筹 | * 环保众筹项目中，为使物联网设备测得的环保指标客观公正，可以采用预言机技术来加强测量结果的可信性 | 基础识记 | 中 | 低 |
| 11.2航空延误险 | * 在航班延误险项目中，其理赔的业务逻辑是事件驱动的 | 基础识记 | 中 | 低 |
| 11.3集会 | * 在集会项目中，为防止来参加集会的人只是过来签个到，中间完全不参加集会从而难以起到预期的产品宣传效果，特安排在集会过程中最多每人签两次到，两个时点都签到才有效。签到时点如何安排，可以让志在必须拿奖的参与者在活动中的平均停留时间最长？答：两个签到时点均随机确定 | 基础识记 | 中 | 低 |
| 11.4文件下载 | * 在文件下载中利用智能合约 | 基础识记 | 低 | 低 |
| 11.5车位共享 | * 在车位共享中利用智能合约 | 基础识记 | 低 | 低 |
| 12. 智能合约的图灵完备性 | 12.1 图灵机模型 | * 图灵奖是计算机科学界的最高荣誉 * 阿兰·图灵是计算机科学的鼻祖，二次大战期间英军的密码专家，并且是强人工智能的判别标准——图灵测试的提出者 * 图灵机模型中含有读写头、状态机和两端无限延伸并可读可写的带子 | 基础识记 | 高 | 高 |
| 12.2 图灵完备性与图灵机停机问题 | * 如果一个系统和装置理论上的计算能力和图灵机这个理论模型的能力是等价的，我们就称这个系统或装置是“图灵完备的(Turing Complete)" * 图灵机停机问题的不可判定性定理说的是：不存在这样的图灵机，它可以可以判定任意一台给定的图灵机是否永不停机 | 一般理解 | 高 | 高 |
| 12.3 智能合约与资源控制 | * 以太坊的智能合约是图灵完备的 * 以太坊引入GAS,用经济手段解决资源控制的数学难题 | 基础识记 | 中 | 低 |
| 12.4 智能合约设计的形式化方法 | * 智能合约设计的形式化方法：开发->测试->形式化验证->部署上线 | 基础识记 | 中 | 低 |
| 13. 激励机制与模型 | 13.1比特币的激励机制 | * 在比特币社区中，率先把一个最新区块挂接到原有区块链中并得到社区确认的人会得到挖矿奖励 * 比特币区块链使用的激励模型是一个通缩模型，每产出210000个区块，它的挖矿奖励数额就减半 * 比特币的挖矿难度是自适应调整的，调整目标是不管挖矿设备和挖矿技术如何进步，出块间隔会被控制在每10分钟左右出一个块的水平 * 挖矿激励是比特币总量增加的唯一来源 | 基础识记 | 高 | 高 |
| 13.2以太坊的激励机制 | * 以太坊上，矿工付出算力，产出交换价值；码农付出智力，产出使用价值 * 每个项目得到一定数量的以太币支持，由码农开发出来应用，可以直接对接现实世界的服务，有明确的使用价值 | 基础识记 | 低 | 低 |
| 13.3 EOS的激励机制 | * EOS 超级节点面向社区开放招商，向超级节点投入资金，除享受优先记账权外，还享有其他受益分享权 | 基础识记 | 低 | 低 |
| 14. 虚拟货币 | 14.1 虚拟货币的一般特点 | * 虚拟货币一般来说地址是公开透明的，而身份是隐匿的。 * 虚拟货币一般在私人机构或民间组织运营的平台上发行 * 虚拟货币一般采用全球联网、社区化运营的方式，在社区成员间流通 | 基础识记 | 高 | 低 |
| 14.2虚拟货币作为支付手段 |  | 不做要求 | 低 | 低 |
| 14.3虚拟货币作为汇兑手段 |  | 不做要求 | 低 | 低 |
| 14.4虚拟货币作为资产计价手段 |  | 不做要求 | 低 | 低 |
| 14.5虚拟货币的意义 | * 长远看，虚拟货币的正常功能都会被法定数字货币或稳定币取代 * 虚拟货币的财产属性一般得到各国法律的认可。以虚拟货币为目标的盗窃、抢劫、勒索行为被普遍认为是犯罪行为 | 基础识记 | 高 | 低 |
| 15. 矿机与钱包 | 15.1矿机 | * 虚拟货币公链上，以获得激励为目的的竞争性记账行为，称为“挖矿” * 最初的区块链上，挖矿是通过软件插件进行的 * 在区块链中，采用哈希勾稽关系把数据记录组织成相互链接的区块，关键在于从对哈希值的约束来反向计算随机配数的值 * 随着虚拟货币的价值飙升，对挖矿技术的升级变得有利可图，面向挖矿的专用硬件开始问世，这就是“矿机“ * 集约化部署矿机的数据中心，被称为“矿场“ * 矿池可以通过集约化的技术架构和紧耦合的协同架构，进一步降低挖矿成本，与矿工之间可以以利益为纽带，建立更密切的商业协同关系。但是，矿池并不能仅仅通过算力的协同来发现挖矿的深层次规律和捷径，目前也不存在通过人工智能发现挖矿规律和捷径的事例 | 基础识记 | 高 | 低 |
| 15.2数字钱包 | * 核心功能：1.存储功能 2. 查询功能 3. 支配功能 * 数字钱包分为热钱包和冷钱包 * 热钱包的优点是操作方便，缺点是安全风险较高；冷钱包的优点是安全，缺点是不方便 | 基础识记 | 中 | 低 |
| 16. 商圈币与积分 | 16.1商圈币 | * 购买商圈币的本质是预付费 * Q币、游戏币、体锻卡、美容卡甚至月饼票、大闸蟹票等等，一旦数字化，都属于商圈币的范畴 * 商圈币流通的实质为从预付费中扣缴消费额 * 特征：商圈币只能在指定范围内流通， 商圈币与法定货币的汇率为1:1，商圈币不得反向兑换为法定货币 | 一般理解 | 高 | 低 |
| 16.2积分 | * 积分源于对消费行为的奖励 | 一般理解 | 低 | 低 |
| 16.3通证经济 | * ”通证经济”涉及资产使用/消费权和所有权、受益权在凭证上的分离 | 一般理解 | 低 | 低 |
| 17. 稳定币 | 17.1什么是稳定币 | * 稳定币是与货币资产或等值的实物资产汇率挂钩的数字货币 * 按挂钩方式分类，稳定币可分为货币资产抵押型、实物资产抵押型和算法盯市型 * 无杠杆型的稳定币发行时需抵押100%的保证金储备 | 基础识记 | 高 | 低 |
| 17.2稳定币USDT（泰达币） | * 稳定币USDT由区块链公司 Tether发行，它的技术体系主要承袭自比特币 * 优点：对于法定货币端的合规性有比较周全的考虑。缺点：运作不够透明 | 基础识记 | 低 | 低 |
| 17.3稳定币 Libra | * Libra由脸书为盟主的包含诸多大型社交媒体、金融机构、电商和其他机构在内的联盟发起。 * Libra的合约编程语言MOVE的特点是在编译的环节就通过强制类型检查来支持价值守恒 * Libra的诉求：（1）无国界（2）点对点（3）可编程（4）零手续费（5）低波动 | 基础识记 | 高 | 低 |
| 17.4中国的应对 | * 法定数字货币 | 基础识记 | 低 | 低 |
| 18. 法定数字货币 | * 1. 什么是法定数字货币 | * 法定数字货币是由各国央行发行的、具有法律规定的货币地位的数字货币 * 最大特点：货币的“法偿性”是指法律规定的不得拒收的支付权利 * 法定数字货币的法律地位等同于现金，属于M0范畴 | 一般理解 | 高 | 低 |
| 18.2中国的法定数字货币 DC/EP | * 中国的法定数字货币 DC/EP: 主要是面向支付环节的数字化工具 * 采用“两库，三中心”技术架构 | 基础识记 | 高 | 低 |
| 18.3后法定数字货币时代的区块链技术 | 随着DC/EP的推出，中国区块链技术领域预期如下积极变化：   * “中国公链”将会起步 * 银行业会被DC/EP激活 * 商家会顺应DC/EP法尝性的要求，推出与DC/EP相配套的一系列举措 * 客户端会通过钱包 APP等方式，使得DC/EP支付应用形成闭环，并与商业银行ATM机业务形成对接 * 区块链学术研究会呈现进一步繁荣景象 * 区块链外围服务将率先出现井喷式爆发 | 一般理解 | 低 | 低 |
| 19. 数字资产交易：中心化模式 | 19.1资产交易总览 | * 标准化的资产可以在传统资本市场交易，比如股票、债券、期货 * 数字化资产交易有两层含义：其一是传统资产借助区块链的技术平台进行交易；其二是区块链上登记的数字资产本身的交易 * 交易所对交易效率的追求体现在吞吐率、时延两大指标上 * 交易所对交易安全的追求体现在RTO(可容许交易中断时间）和RPO（可容许交易数据丢失间隔）两大指标上 | 一般理解 | 高 | 低 |
| 19.2交易机制分类 | * 订单交叉指最低卖价低于最高买价的现象，订单簿交叉是交易得以进行的根本动力掌握Series对象的创建 * 交易机制分类：1.订单驱动交易机制 2.报价驱动交易机制 * 订单驱动交易机制： 集合竞价机制 、连续竞价机制 * 报价驱动交易机制一般采用场外市场方式组织(OTC) | 基础识记 | 高 | 低 |
| 19.3订单驱动交易机制介绍 |  | 不做要求 | 低 | 低 |
| 19.4报价驱动的交易机制介绍 |  | 不做要求 | 低 | 低 |
| 19.5数字资产交易的区块链实现 |  | 不做要求 | 低 | 低 |
| 20. 数字资产交易：去中心化模式 | 20.1链上资产中心化交易模式的弊端 | * 数字资产交易的模式有中心化模式、传统交易所模式和去中心化模式 * 中心化交易所的模式：由一家市场化的实体公司发起，交易订单通过统一的域名入口接入交易系统，交易系统代码以及交易细节对外不公开，对用户充入这家交易所的数字资产，这家交易所拥有最终控制权 * 去中心化交易所：由一个社区发起，凭借现有的公链或自建的公链，通过链上智能合约实现交易功能并提供交易服务，交易的细节可以向用户披露并接受用户的监督。 | 一般理解 | 高 | 低 |
| 20.2去中心化交易模式的探索 | * 实现去中心化交易模式的途径：1. 链内加速 2. 链外加速 3. 交易后处理剥离 | 基础识记 | 低 | 低 |
| 20.3“撮合即挖矿”交易模式简介 | * “撮合即挖矿”的核心思想是把交易撮合用竞争性挖矿的方式可检验地放在插件上 | 基础识记 | 高 | 低 |
| 21. 供应链金融 | 21.1问题的提出 | * 根据资本市场的“倒金字塔”现象，广大小微企业不存在从资本市场获得投资的可能性 * 依托于核心企业采购供应链的小微企业，虽有最终来自核心企业的应收账款作为未来现金流，但由于处在供应链末端，信用无法穿透 * 小微企业之所以周转难，是因为体量小、账期长、很多情况下需要外部资金环节压力 * 核心企业采购供应链这一构成优质小微企业“结构性依托”的要素没有被揭示和识别出来，导致无论是间接融资还是直接融资，都不乏对待小微企业“一刀切”的排斥现象 | 一般理解 | 高 | 低 |
| 21.2区块链解决方案 | * 基于区块链的采购供应链融资解决方案，应解决如下几个问题： * 提供可信的应收账款信息 * 沿采购供应链逐级穿透直至末端 * 提供可质押的帅化权益证明 * 在区块链领域，IOU(I owe you) 既是应收账款作为待披露事实的载体，也是采购方逐级授信的载体，同时还是可质押的权益证明的载体 | 一般理解 | 高 | 低 |
| 21.3衍生服务与启示 | * 对于资本市场而言，采购供应链融资的区块链解决方案最大的好处就在于揭示了这些小微企业的投资价值。 * 在区块链所记载的应收账款历史记录的基础之上，还可以催生出另外一些服务形态，比如说信用评级 | 一般理解 | 低 | 低 |
| 22. 信用证与R3 | 22.1信用证简介 | * + 信用证（Letter of Credit，英文简称LC），是交易双方借助各自的开户银行对货款兑付的一种信用担保凭证   + 信用证业务的参考流程：1.合同 ->2.申请开证 -> 3.开立信用证 -> 4.通知信用证 -> 5.装货 -> 6. 交单 -> 7.议付押汇或收妥结汇 -> 8.寄单索偿 -> 9.审单付账 -> 10. 提示付款 -> 11. 付款赎单 ->12.凭单提货 | 基础识记 | 高 | 低 |
| 22.2信用证的区块链实现 | * + 传统方式进行信用证单据的真伪识别“痛点”：花费大量人力物力、形成效率瓶颈、蕴含巨大的风险   + 在信用证业务中，传统纸质单据防伪的“哑铃状罩门”指的是标的面值高、鉴别成本高、造假成本低   + 在信用证业务中，纸质单据丢失往往被视为“不可抗力”，也出现过相关条款被恶意使用的情形   + 区块链技术实现信用证业务，意味着单据在流程中的直通。在区块链与物联网深度结合的情况下还可以码随货走，验码即验货。这会大大节约总体成本，大大提高交易安全性 | 一般理解 | 高 | 低 |
| 22.3 R3 Corda 简介 | * + R3 Corda被R3定位为受区块链启发的技术平台，而不是通常意义上的区块链   + R3 Corda “单据驱动的流程自动化”参考架构，单据在账本层进行可靠存证，前序单据作为合约的“要件”输入合约   + 合约的执行结果必须经过“公证人”节点的共识背书方可生效   + 合约的自然语言文本作为合约的不可分割的组成部分，其哈希值嵌入合约，原件由存储服务保存，发生争议时以文本为准 | 一般理解 | 中 | 低 |
| 23. 数据交易 | 23.1数据交易是伪命题吗 | * + 数据买卖的主观需求和数据交易的客观制度安排都没有障碍，但数据权益保护的技术手段不足，导致数据扩散无法控制，会侵害数据交易者的利益   + 数据交易产业的现状：数据泄露的丑闻频发，对数据的滥用状况十分令人担忧；数据的主人权益意识不足，对自身数据的价值认识也不足；数据的交易渠道不畅，事实上的数据黑产已经形成； 数据权益保护的法律环境还不完善   + 因为数据可以带来增量价值，数据已经从一般意义上的“资源”变成了“资产” | 基础识记 | 高 | 低 |
| 23.2数据交易的区块链解决方案 | * 在数据交易的区块链解决方案中，如果数据交易与支付既要实时连动，又要体现买方对资金的支配权，应该把一部分资金打入智能合约以便备付   + 调用和交易的明细，以存证的方式记录在区块链上。如果区块链和法定数字货币连动，则可以直接通过法定数字货币向服务提供者付费 | 基础识记 | 高 | 低 |
| 23.3数据交易的价值 | * + 数据交易有明显的增值作用   + 数据是宝贵的资源和资产。数据的无节制滥用亟须改变。区块链可助力数据交易，而数据交易的持续发展和应用深入，仍面临着不少技术挑战   + 数据交易的技术挑战：1.隐私保护问题。2. 再授权问题。3. 数据销毁问题 | 基础识记 | 中 | 低 |
| 24. 区块链防伪：存证、溯源与确权 | 24.1 存证 | * + 在纵向垂直管理体系当中，上级为什么也需要间接下级使用基于区块链的存证服务？因为上级可以对间接下级的工作结果实行穿透式留痕   + 本教材所提出的区块链八层结构中，实现存证+定序服务功能只需用到下面4层：不可篡改、不可仿冒、不可抵赖、不可乱序   + 区块链提供基于密码学原理的存证+定序功能，更加可靠，同时在技术上与支付的衔接更加紧密 | 基础识记 | 高 | 低 |
| 24.2溯源 | * + 对物品的流通路径进行可验证、可追溯、可信赖的数字化表示，称为溯源   + 物品的流通一般都会经过很多环节，从原产地到运输、中间经销商再到零售，每个环节都有可能混入不可信因素，构成对物品流通历史的造假。溯源的目的是证明每个流通环节的真实性，提供系统化的、前后一致的防伪证据 | 基础识记 | 高 | 低 |
| 24.3 确权 | * + 以数字化的方式见证一种权利的成立，就是“确权” | 基础识记 | 低 | 低 |
| 25. 一切皆挖矿：共享资源的社区化模式 | 25.1算力挖矿的启示 | * + 算力挖矿本身已经进入尾声   + 算力挖矿带给我们的一个具有广泛共性的启示是，它建立了一个贡献-检验-激励的良性循环。在算力挖矿的模式下，贡献是可检验的，检验是跟激励绑定的，而激励则导向可持续的贡献。这个“贡献-检验-激励”的良性循环，才是值得我们下大力气去挖掘、推广并发扬光大的 | 基础识记 | 高 | 低 |
| 25.2挖矿激励的共性原理 | * + 贡献和检验难度不对称, 既是挖矿激励模式成立的先决条件，同时也是具有足够普遍性的一种现象 | 基础识记 | 低 | 低 |
| 25.3挖矿激励的案例分析 | * + 存储挖矿，如IPFS   + 缓存挖矿，如迅雷。所谓CDN指的是缓存分配网络（Content Distribution Network）   + 资源建设众包挖矿，如词典编撰   + 计算挖矿，如数据联邦   + 交易引擎共享模式，“撮合即挖矿”的核心思想就是把交易撮合用竞争性挖矿的方式实现在插件上，供交易参与者公开检验 | 基础识记 | 低 | 低 |
| 26. 区块链+开源数据库≥商业数据库 | 26.1 区块链不是数据库 | * + 数据库的标配功能。创建（Create）读取（READ）修改（Update）删除（Delete) CRUD   + 区块链只能做到C和R，做不到U和D   + 关于区块链与数据库的关系，（1）区块链根本不是数据库；（2）区块链不应该当数据库用；（3）区块链跟数据库不可比   + UTXO可被视为操纵数据的指令 | 基础识记 | 高 | 低 |
| 26.2 商业数据库与开源数据库的比较 | * + 商业数据库在原子性事务、回滚、高可用同步等方面有着独特优势   + 开源数据库在开源基金会的支持下，由开源社区主导开发、供用户机构在遵守开源协议前提下免费使用   + 仅靠开源数据库，用户无法享受到商业数据库所提供的异常场景下的专业、鲁棒的服务水准 | 基础识记 | 低 | 低 |
| 26.3 区块链+开源数据库解决方案 | * + 智能合约通过状态机模型将事务的执行状态在区块链基础账本上存证，所以从区块链基础账本中看到的事务就是原子化的   + 与区块链相耦合的开源数据库，可以把重点放在查询和数据分析等方面的高性能支持上 | 基础识记 | 高 | 低 |
| 26.4 去中心化的中台 | * + 去中心化的中台 通过区块链的赋能，在企业级存证与回放技术设施的基础上，进一步把存证与回放的服务延展到多方参与的联盟链场景。 | 基础识记 | 低 | 低 |
| 27. 隐私保护：场景 | 27.1 隐私保护的定义和意义 | * + 隐私保护技术：在多方业务往来中，控制己方拥有的数据主权的数据使其不为其他方所知晓，同时又不影响业务进行的技术   + 隐私保护与区块链之间的关系：绝大多数现有的区块链系统中并不包含隐私保护的功能 | 基础识记 | 高 | 低 |
| 27.2 区块链隐私保护的目标冲突 | * + 仅凭地址匿名机制，现有区块链公链并不能很好地保护用户隐私   + 联盟链，其加盟方希望隐私保护技术即使实现，也要依托某种去中心化的机制实现，不能把隐私保护的实现寄托在对哪一个特点节点的无条件信任之上 | 基础识记 | 低 | 低 |
| 27.3 隐私保护的场景举例 | * + 四种隐私保护场景：1.背靠背比对 2.背靠背查询 3. 背靠背评分 4. 背靠背聚合 | 基础识记 | 高 | 低 |
| 27.4 隐私保护技术的发展路径 | * + 发展三步：1. 提供基本匿名性服务 2.提供有限的、局部的隐私保护功能 3.实现全面彻底隐私保护功能。 我们目前处于从第二步向第三步过渡阶段 | 基础识记 | 低 | 低 |
| 28. 隐私保护：技术原理 | 28.1 概要介绍 | * + 何谓隐私保护的“不可能三角”？去中心化程度、隐私保护、性能不可兼得   + 隐私保护技术的坐标图维度：横轴 - 隐私性由弱到强，竖轴 - 中心化由强到弱 | 基础识记 | 高 | 低 |
| 28.2 有限、局部的隐私保护技术 | * + CCP 方案、状态通道方案(state channel)、 Tear-off 方案在隐私保护坐标图上的位置 | 基础识记 | 中 | 低 |
| 28.3 全面、彻底的隐私保护技术 | * + 零知识证明、同态加密、联邦学习 | 基础识记 | 高 | 低 |
| 29. 隐私保护：应用案例 | 29.1 交易后业务处理 | * + 在交易后业务处理的区块链解决方案中，多边联合记账的主要障碍来自各个市场机构的法定职能边界   + 在交易后业务处理的区块链解决方案中，隐私保护诉求防范的是其他证券公司 | 基础识记 | 高 | 低 |
| 29.2 供应链溯源 | * + 在溯源场景中进行隐私保护的主要诉求来自中介商 | 基础识记 | 高 | 低 |
| 29.3 采购供应链融资 | * + 在采购供应链融资场景中隐私保护的诉求，公司不希望透露上下游合作方、IOU分拆细节 | 基础识记 | 中 | 低 |
| 29.4 背靠背求交集 | * + “背靠背求交集”的区块链解决方案中每方的区块链节点都部署在己方可控区域自主运营，而不是部署在第三方区域由第三方运营 | 基础识记 | 中 | 低 |
| 29.5 跨越边界的协同计算 | * + 医院与保险公司协同合作，利用区块链平台进行协同计算 | 基础识记 | 中 | 低 |
| 29.6 隐私货币 | * + 零币Zcash是世界上第一个使用零知识证明技术的虚拟数字货币   + 达世币Dash使用了独特的混币技术   + 门罗币区块链使用了环签名技术 | 基础识记 | 中 | 低 |
| 30. 跨链技术 | 30.1 基本概念 | * + 在两个不同的区块链之间传递价值和信任状态的机制，称为“跨链”   + 跨链有两个根本要求：1. 两个链间价值守恒 2. 两个链间时间同步。两点依赖于一个前提：两个链之间的互认   + 为什么会有区块链跨链的需求？因为一条区块链不应该与其他区块链隔绝，成为证据和价值的孤岛   + 实现跨链和实现两个IP网络之间互联互通，最大的不同在哪里？实现不同链上价值和信任状态的互联互通 | 基础识记 | 高 | 低 |
| 30.2 跨链技术方案与项目 | * + 最简单的跨链就是主链和侧链的交互   + 平等关系的跨链技术主张分两派：中介链方案和转接协议方案 | 基础识记 | 中 | 低 |
| 30.3 可能的演化方向与问题 |  | 不做要求 | 低 | 低 |
| 31. 性能优化 | 31.1计算 | * + 区块链上交易达成的三个阶段：1.存证和定序 2.业务有效性检验 3.业务处理及最终结果入账。   + 计算性能优化方向：1. 流水 2.分片 3.链外加速 | 基础识记 | 高 | 低 |
| 31.2存储 | * + 存储优化方案：分片和快照 | 基础识记 | 中 | 低 |
| 31.3共识 | * + 共识机制三种类型：基于证明的、基于投票的、基于随机性的   + 共识机制优化趋势：节点从多到少、拓扑从链到图、确定性从确定到随机 | 基础识记 | 高 | 低 |
| 32. 关于区块链的误区种种 | 32.1 去中心化是区块链的本质属性？ | * + 去中心化不是区块链的本质属性 | 一般理解 | 低 | 低 |
| 32.2 区块链不能没有自己的 币？ | * + 区块链可以没有自己的币 | 一般理解 | 低 | 低 |
| 32.3 区块链可以不开源？ | * + 区块链需要开源 | 一般理解 | 低 | 低 |
| 32.4 区块链行业可以产生独角兽？ | * + 区块链行业投资价值 | 一般理解 | 低 | 低 |
| 32.5 做区块链只需简单业务搬家？ | * + 做区块链不能只需简单业务搬家 | 一般理解 | 低 | 低 |
| 32.6量子计算将终结区块 链？ | * + 量子计算对区块链的影响 | 一般理解 | 低 | 低 |
| 32.7 区块链公开透明，无法 保护隐私？ | * + 区块链公开透明，无法保护隐私的理解不对 | 一般理解 | 低 | 低 |
| 32.8 区块链用的现成技术， 没有技术创新？ | * + 区块链集成创新 | 一般理解 | 低 | 低 |
| 33. 区块链的安全、运维和治理 | 33.1区块链的安全 | 安全问题”三分技术，七分管理”。安全管理关联到责任，区块链本 身的特点决定了安全责任落实并不简单   * + 社区管理，没有强制性安全基线管理和强制性安全检查   + 发生技术安全连带业务损失，职责边界不易界定   + 联盟链跨机构甚至跨境部署，机构之间的安全域划分不易区分   + 密码学相关安全问题，如量子计算技术 | 基础识记 | 高 | 低 |
| 33.2区块链的可运维性 | * + IT系统的可运维性，指的是该系统自身所提供的确保该系统的正常运行状态、排除该系统的异常运行状态、应对突发的运行需求的能力。   + 金融行业，确保系统的正常运行状态的主要途径是架构手段，即通过高可用架构实现尽量短的故障恢复时间目标（RTO）和可容忍故障恢复点目标（RPO）   + 在金融行业，应对突发的运行需求的主要途径，在架构层面是参数化设计，在操作层面是保留最终干预权   + 区块链技术领域可运维性的两个努力：1. 埃森哲公司提出的“可编辑的区块链”概念。2.R3联盟推出的 Corda 平台，智能合约代码和对应该合约的正式有效的法律文本相互勾稽。 | 基础识记 | 高 | 低 |
| 33.3区块链的治理 | * + 区块链社区遇到不能达成共识的情况的应对：分叉   + 国家层面看待区块链行业的治理，要有明确的分类监管原则：1.链圈应在合规前提下鼓励创新。2.币圈自身应用不涉及资本市场叠加应用的适度监管。3.对于与资本市场叠加应用的，严格监管。 | 基础识记 | 低 | 低 |
| 34. 区块链产业及投资前景分析 | 34.1区块链产业的特点 | * + 产业特色：以技术为驱动，以信任为标的，以极客为载体，以价值为激励 | 基础识记 | 中 | 低 |
| 34.2区块链产业的现状 | * + 区块链产业的现状：1.信息不对称严重 2.技术迭代周期短，速度快 3.政策性强，监管不确定性大 4. 许多职能缺位 | 基础识记 | 高 | 低 |
| 34.3区块链产业的新机遇 | * + 新形势下，投资决策考量应主要侧重聚焦的场景、落地能力、稳定的团队和稳健合规的经营。 | 基础识记 | 低 | 低 |
| 35. 区块链落地方法论 | 35.1区块链的比较优势和比较劣势 | * + 比较优势：多方参与、自证清白、增量业务   + 比较劣势：1. 过于冗余的资源消耗。2. 对已有可信资源的利用不足 | 基础识记 | 高 | 低 |
| 35.2记账权、监督权与使用权 | * + 区块链上的权限：使用权、监督权、记账权 | 基础识记 | 高 | 低 |
| 35.3发行与流通 | * + 发行功能对于区块链来说只是一个可选项   + 区块链的流通功能是构成未来价值互联网的基石 | 基础识记 | 低 | 低 |
| 35.4底层账本与智能合约 | * + 使用区块链提供的底层账本对于智能合约来说只是一个可选项   + 把智能合约建立在开放银行API基础上也是一种选择 | 不做要求 | 低 | 低 |
| 36. 区块链前沿应用领域 | 36.1 区块链与NFT（非同质化通证） | * NFT的基本概念 * NFT的发展历程 * 数字化原生物品的NFT * 非数字化物品的NFT * NFT的铸造、流通与销毁 * NFT与区块链技术 | 一般理解 | 中 | 低 |
| 36.2 区块链与元宇宙 | * 元宇宙的基本概念 * 元宇宙的发展历程 * 元宇宙的技术体系 * 元宇宙中的稀缺性技术 * 元宇宙中的工业互联网 | 一般理解 | 低 | 低 |
| 36.3 区块链与Web3.0 | * Web3.0的基本概念 * Web3.0的发展历程 * Web3.0的典型特征，与Web1.0和Web2.0联系与区别 * Web3.0与区块链技术 * Web3.0与隐私计算 | 一般理解 | 低 | 低 |
| 37. 区块链技术发展前景展望 | 37.1 线路图：数字化与治理 | * + 区块链技术及其应用的未来发展路径 -- 两个维度：治理模式（横轴）、数字化水平（纵轴）   + 数字化平台建设、受区块链启发的解决方案、区块链完备的解决方案、增强的区块链解决方案 | 一般理解 | 高 | 低 |
| 37.2 价值互联网与未来区块链生态 |  | 不做要求 | 低 | 低 |
| 37.3 区块链与其他新兴技术的对接 |  | 不做要求 | 低 | 低 |
| 37.4 可以期待的变化 |  | 不做要求 | 低 | 低 |

## 重要高频考点题目

* 区块链技术的应用价值
* 比特币与区块链1.0
* 区块链技术的三大支柱技术
* 比特币创新
* 密码学里的基本场景设定
* 密码学定义
* 对称加密机制的优点
* 非对称加密机制的正向使用、反向使用
* 拜占庭容错
* 非信任环境中的信任服务基础设施
* 区块链核心功能、业务功能
* 区块链在币圈的应用
* 区块链在链圈的应用
* NFT（非同质化通证）

# 历年真题与考试样题

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 题面 | A | B | C | D | 正确答案 |
| 信任的对象应包括（ ）。 | 当事对方 | 当事对方、中介人 | 当事对方、中介人、中介机构 | 当事对方、中介人、中介机构、数学或算法 | D |
| 是什么造就了区块链技术的应用价值？（）。 | 无与伦比的安全性 | 信任路径的再定义能力 | 强大的共识机制 | 不可篡改的数据组织方式 | B |
| 以下技术，哪一个不属于区块链技术的三大支柱技术？（）。 | 分布式系统 | 对等网络 | 图论 | 密码学 | C |
| 用于信息的存证、防伪和高忠实度浓缩表示的密码学技术是（）。 | 哈希 | 对称加密 | 非对称加密 | 零知识证明 | A |
| 每个参与方都知道的密钥是（ ）。 | 公钥 | 私钥 | 对称密钥 | 非对称密钥 | A |
| 在公钥签名当中，约定收发双方使用同样的哈希函数的原因是（ ）。 | 避免双方对同样的原文，产生不同的哈希值 | 避免双方对原文出现理解上的歧义 | 避免双方系统不兼容 | 避免双方签名-检验环节中出现异常 | A |
| 分布式系统是通过\_\_\_\_\_连接在一起的若干台（ ） | 网络，路由器 | 路由器，计算机 | 网络，计算机 | 计算机，路由器 | C |
| 一个分布式系统的全局工作状态称为一个（ ）。 | 资源 | 节点 | 副本 | 进度 | C |
| 比特币之前的区块链研究，共同特点是（ ）。 | 没有摆脱对于可信第三方的依赖 | 没有引入工作量证明的机制 | 没有使用非对称加密 | 没有引入POW共识机制 | A |
| 区块链通过采用独特的数据组织方式，在（ ）中实现了时间不可逆性？ | 物理世界 | 信息世界 | 社会生活 | 精神世界 | B |
| 就构建“价值互联网”这一愿景而言，价值与信息最根本的不同是（ ）。 | 信息可以是不真实的，价值必须是真实的 | 信息可以是不安全的，价值必须是安全的 | 信息可以是不守恒的，价值必须是守恒的 | 信息可以是不可用的，价值必须是可用的 | C |
| 在区块链中，依靠（ ）参与见证，用事先确定的（ ）对见证的结果进行综合，最终达成被所有参与者认可的共识结论的机制，称为共识机制。 | 权威，节点 | 群体，规则 | 规则，权威 | 规则，群体 | B |
| PBFT算法形成于（ ）年。 | 1989 | 1999 | 2009 | 1979 | B |
| 一个区块链如果仅含基础账本，以下的哪一个表述不属于它的不足之处？（）。 | 不能对外界变化做出实时反应 | 不能包含复杂的业务逻辑 | 不转账就不流动，不能充分发挥数字化世界的特点 | 不具有图灵完备性 | D |
| 在环保众筹项目中，为使物联网设备测得的环保指标客观公正，可以采用（ ）技术来加强测量结果的可信性 | 人工智能 | 大数据 | 云计算 | 预言机 | D |
| 以下哪个身份不适合阿兰·图灵？（）。 | 计算机科学的鼻祖 | 二次大战期间英军的密码专家 | 强人工智能的判别标准——图灵测试的提出者 | 信息论的创始人 | D |
| （ ）是比特币总量增加的唯一来源。 | 外部注入 | 跨链转账 | 挖矿激励 | 交易所购买 | C |
| 虚拟货币一般来说（ ）是公开透明的，而（ ）是隐匿的。 | 身份、账目 | 账目、身份 | 地址、账目 | 身份、地址 | B |
| 在区块链中，采用哈希勾稽关系把数据记录组织成相互链接的区块，关键在于从对哈希值的约束来反向计算（ ）的值。 | 随机配数 | 本区块的哈希树根 | 上一区块的哈希值 | 本区块的工作载荷 | A |
| 下列说法中哪一个是错的？（）。 | 商圈币与法定货币的汇率为1:1 | 商圈币只能在指定范围内流通 | 商圈币可以反向兑换为法定货币 | Q币、游戏币、体锻卡、美容卡甚至月饼票、大闸蟹票等等，一旦数字化，都属于商圈币的范畴 | C |
| “稳定币”指的是（）。 | 可交易的商圈币 | 法定数字货币 | 与货币资产或等值的实物资产汇率挂钩的数字货币 | 与比特币汇率挂钩的虚拟货币 | C |
| 法定数字货币的发行者是（）。 | 商业银行 | 民间机构 | 各国央行 | 跨国货币组织 | C |
| 以下各类资产，哪一个不可以在传统资本市场上交易？（）。 | 股票 | 债券 | 期货 | 大宗商品 | D |
| 数字资产交易有哪几种模式？（）。 | 中心化模式 | 中心化模式、去中心化模式 | 中心化模式、传统交易所模式、去中心化模式 | 中心化模式、传统交易所模式 | C |
| 小微企业之所以周转难，以下哪一个不属于原因之一（）。 | 体量小 | 账期长 | 很多情况下需要外部资金环节压力 | 信誉差 | D |
| 信用证是交易双方借助各自的开户银行对（ ）的一种信用担保凭证 | 价格公平 | 商品质量 | 商品真伪 | 货款兑付 | D |
| 为什么说数据已经从一般意义上的“资源”变成了“资产”？（）。 | 因为数据可以解决问题 | 因为数据可以吸引投资 | 因为数据可以带来增量价值 | 因为数据可以折算成无形资产 | C |
| 本教材所提出的区块链八层结构中，实现存证+定序服务功能只需用到下面（ ）层。 | 2 | 3 | 4 | 5 | C |
| 算力挖矿本身已经进入（）。 | 前期 | 中期 | 后期 | 尾声 | C |
| 用数据库的CRUD功能特性来衡量区块链，区块链能做到哪些？（）。 | C | CR | CRU | CRUD | B |
| 下列说法中哪一个是错的？（）。 | 数据的滥用现象非常严重，发展隐私保护技术适逢其时 | 用让渡部分隐私换取方便是值得的，中国人不需要隐私保护 | 许多业务，不解决隐私保护问题就没法开展 | 许多隐私保护需求，离开了区块链的辅助就无法满足 | B |
| 何谓隐私保护的“不可能三角”？（）。 | 去中心化程度、隐私保护、可扩展性不可兼得 | 去中心化程度、性能、可扩展性不可兼得 | 去中心化程度、隐私保护、性能不可兼得 | 性能、隐私保护、可扩展性不可兼得 | C |
| 在交易后业务处理的区块链解决方案中，隐私保护诉求防范的是（ ）。 | 交易所 | 登记结算机构 | 其他证券公司 | 普通投资者 | C |
| 为什么会有区块链跨链的需求？（）。 | 因为一条区块链不能包办所有的信任服务 | 因为一条区块链不能覆盖所有的客户群体 | 因为一条区块链不能无视其他区块链上已经存在的证据和价值 | 因为一条区块链不应该与其他区块链隔绝，成为证据和价值的孤岛 | D |
| 最不利于发挥流水方式并行加速优势的场景是什么？（） | 工序太多 | 工序太少 | 工序间通信太频繁 | 工序间工作负载太不均衡 | D |
| 以下各论述，哪一条不构成支持“去中心化不是区块链的本质特征”的论据？（）。 | 去中心化的初衷不一定带来去中心化的演化趋势和结果 | 去中心就是不要监管，这是无政府主义 | 去中心不等于去监管，该表述容易引起误解 | 在合适的场景针对合适的权限引入中心化要素，可以更加符合实际需求 | B |
| 哪三个因素的叠加，导致EOS平台一度出现严重的安全问题？（）。 | 软件本身的缺陷，服务器的同质化，记账节点的数目过少 | 软件本身的致命缺陷，记账节点的数目过少，记账节点随机产生 | 服务器的同质化，记账节点的数目过少，专业安全公司的努力 | 软件本身的致命缺陷，安全公司的努力，记账节点的数目过多 | A |
| 下列各项陈述中，哪一个没有反映区块链产业的特点？（）。 | 以股权为激励 | 以技术为驱动 | 以极客为载体 | 以信任为标的 | A |
| 为什么区块链更适合多方参与的场景？（）。 | 因为多方参与需要多台设备 | 因为多方参与需要多套数据 | 因为多方参与需要对接多套存量系统 | 因为利益取向不同的多方参与，需要建立为各方所信任、在各方参与和监督下能够做到技术中立的平台 | D |
| “区块链完备的解决方案”意味着（）。 | 数字化水平已经不低，但是治理的去中心化程度有待提高 | 数字化水平有待提高，但治理的去中心化程度已经不低 | 数字化水平和治理的去中心化程度都很低 | 数字化水平和治理的去中心化程度都已经不低 | D |