EXIN Blockchain

FOUNDATION

Certified by

考试样卷

202202 版本

目录

考试说明

本试卷是 EXIN Blockchain Foundation (BLOCKCHAINF.CH)模拟考试。 EXIN 考试准则适用于该考试。

本试卷由 40 道单项选择题组成。每道选择题有多个选项，但这些选项中只有一个是正确答案。

本试卷的总分是 40 分。每道题的分数是 1 分。您需要获得 26 分或以上通过考试。

考试时间为 60 分钟。

祝您好运!

考试样卷

1 / 40
哪一项是公有链的优点?

What is an advantage of a public blockchain?

A) 公有链不使用无利害关系的第三方保护区块安全,因为所有参与者都具有既得利益。
It does not use disinterested third parties to secure blocks, as all participants have a vested interest.
B) 公有链具有更强的抵御欺诈能力,因为它使用联盟节点来对抗欺诈。
It is more resilient against fraud, because it uses federated nodes to combat fraud.
C) 公有链对全世界所有人开放,无需许可和授权要求。
It is open to everyone in the world without permission and licensing requirements.
D) 公有链网络由营利性公司构建,网络的正常运行有所保障。
Its networks are built by for-profit companies and the working of the network is guaranteed.

2 / 40
什么是区块链?

What is a blockchain?

A) 一种集中式数据库,存储着所有节点上所有交易记录的子集。
A centralized database that holds a subset of all transactions on all nodes.
B) 一种客户-服务器数据库,数据同时存在于有限数量的节点中。
A client-server database existing on a limited number of nodes at the same time.
C) 一种将所有的交易记录都存储在网络上的分布式数据库。
A distributed database with a record of all transactions on the network.
D) 一种独立运行数据库,由多个节点存储着所有的历史交易记录。
A standalone database with history of all transactions on various nodes.

3 / 40
区块链网络中轻节点的功能是什么?

What is the function of a lightweight node within a blockchain network?

A) 轻节点存储网络上每笔交易的完整历史记录。
It stores a complete history of every transaction on the network.
B) 轻节点为区块链网络的用户存储购买的加密货币。
It stores purchased cryptocurrency for users of a blockchain network.
C) 轻节点通过借用全节点的工作来验证交易。
It verifies transactions by piggybacking on the work of full nodes.

哪一项**不属于**节点的类别?

What is **not** a classification for a node?

A) 全节点
Full node
B) 轻节点
Lightweight node
C) 默克尔节点
Merkle node
D) 矿工节点
Miner node

5 / 40

一种无记名票据可通过区块链网络在两方之间转移价值。

以上说的是哪一种票据?

A bearer instrument used to transfer value between two parties over a blockchain network.

What is this instrument?

A) DApp
A DApp
B) 哈希
A hash
C) 节点
A node
D) 通证
A token

6 / 40

公有链的**关键**特点是什么?

What is a **key** characteristic of a public blockchain?

A) 允许用户选择节点处理交易
Allowing a user to elect nodes to process transactions
B) 允许任何人参与区块链网络
Allowing anyone to participate in the blockchain network
C) 允许控制参与的主体以及参与的级别
Allowing control over who can participate and at what level
D) 仅允许可信方操作其区块链
Allowing only trusted parties to operate their blockchain

哪一项属于密码学在区块链的应用案例?

What is an example of the use of cryptography in a blockchain?

A) 使用私钥访问私有链或混合链
Accessing private or hybrid blockchains by using a private key
B) 创建加密货币作为挖矿节点的奖励
Creating cryptocurrency as a reward for mining nodes
C) 保护区块链免受损坏节点的51%攻击。
Keeping blockchains secure from 51% attacks by corrupt nodes
D) 确保接受者之间加密货币的安全转移
Securing transfers of cryptocurrency between recipients

8 / 40
区块链如何利用私钥和公钥加密?

How do blockchains use private and public-key cryptography?

A) 非对称加密允许发送者将加密货币转移至公钥。然后,接收者可用各自的私钥访问资金并将资金存入钱包。
Asymmetric encryption allows a sender to transfer cryptocurrency to a public key. The recipient can then access these funds with their private key and hold it in their wallet.
B) 在公钥加密中,一个密钥用于对交易进行加密和解密。发送方使用此密钥发送加密货币,而接收方的钱包在解密后保存加密货币。
In public-key cryptography, one key is used to encrypt and decrypt transaction. The sender uses this key to send cryptocurrency and the recipient's wallet holds it after decryption.
C) 对称加密允许发送者向另一个用户传输加密货币。然后,当发送方授予对其私钥的访问权时,接收方可以访问其资金。
Symmetric encryption allows a sender to transfer cryptocurrency to another user. The recipient can then access their funds when the sender grants access to their private key.
D) 区块链中的算法将私钥和公钥加密并存储到所有用户的钱包中。然后,用户通过二十位口令密钥访问其资金。
The algorithm in the blockchain encrypts and stores private and public keys to all user's wallets. The user then accesses their funds through their twenty-word passphrase key.

9 / 40
混合链网络如何对抗51%攻击?

How do hybrid blockchain networks combat 51% attacks?

A) 通过一个中央控制器,确保网络中每个节点的安全
Through a central controller ensuring the security of each node in the network
B) 通过一个工作量证明(PoW)算法,允许矿工保护网络安全
Through a Proof of Work (PoW) algorithm, which allows miners to secure the network
C) 通过激励,矿工通过确保网络安全而获得货币
Through incentivization, where miners receive currency for securing the network
D) 通过默克尔树根,允许网络将自身还原到其最后一个有效区块
Through Merkle tree roots, that allow the network to restore itself to its last valid block

区块链如何像账本一样发挥作用?

How do blockchains function like ledgers?

A) 区块链保留了网络上发生的所有交易的记录。
　　 They hold a record of all transactions that have ever occurred on a network.
B) 区块链将大量交易数据保存为一个中央数据库。
　　 They hold vast amounts of transaction data as a centralized database.
C) 区块链定期更新区块链中每个钱包的所有余额。
　　 They periodically update all balances of each wallet to the blockchain.

区块链网络中矿工的任务是什么?

What is the task of miners in a blockchain network?

A) 矿工作为单一的第三方来收集记录，并通过矿工权威当局向网络提供信任。
　　 Miners act as a single third party to aggregate records and provide trust in the network by the miners' authority.
B) 矿工是允许访问区块链的计算机，确保损坏节点的数量保持较低水平。
　　 Miners are computers that allow access to the blockchain, ensuring the number of corrupt nodes will stay low.
C) 矿工是通过计算正确的随机数促成交易而竞争奖励的节点。
　　 Miners are nodes that compete for a reward by calculating the correct nonce to make a transaction possible.
D) 矿工决定应遵守的共识规则，并在这些规则被打破时进行干预。
　　 Miners determine the consensus rules that should be followed and interfere when these rules are broken.

哪一项描述**仅**符合工作量证明（PoW）共识算法?

Which description fits **only** the Proof of Work (PoW) consensus algorithm?

A) 一种协作共识算法，由被授权的账户执行验证。
A collaborative consensus algorithm, where approved accounts do the validation.

B) 一种由农民推动的协作共识算法，他们提供计算机剩余的内存，使交易成为可能。
A collaborative consensus algorithm that is facilitated by farmers, who offer leftover memory of their computer to make transactions possible.

C) 一种共识算法，对整个交易流程进行验证，包括正确性以及交易顺序。
A consensus algorithm, where the validation is done for the entire transaction flow, including not only the correctness, but also the sequence of transactions.

D) 一种低成本的快速算法，节点需要存入加密货币以担保交易进行。
A low-cost and fast algorithm, where a node needs to deposit cryptocurrency to guarantee the transaction.

E) 一种非竞争性共识算法，验证由选定节点执行，而选定节点将加密货币发送到一个地址，而从这个地址加密货币无法被收回。
A noncompetitive consensus algorithm, where validation is done by elected nodes, which send cryptocurrency to an address, from which it cannot be retrieved.

F) 一种涉及协同验证的算法，协同验证由共识之外选择的验证者执行。
An algorithm that involves collaborative validation, performed by validators, which are chosen outside of the consensus.

G) 一种算法，可在可信执行环境中工作，并证明交易发生的时间。
An algorithm that works in a trusted execution environment and proves the time when the transaction has taken place.

H) 一种高强度且昂贵的竞争性算法，其中区块链上的每个挖矿节点都在相互竞争从而确保其获得区块。
An intensive and expensive, competitive algorithm where each mining node on the blockchain is competing to secure blocks.

一种竞争性共识算法因区块链难以满足交易速度要求而开发。

以上说的是哪一种共识算法?

A competitive consensus algorithm that was developed because blockchains had difficulty meeting the transaction speed demands.

Which consensus algorithm is this?

A) 股份授权证明机制（DPoS）
Delegated Proof of Stake (DPoS)

B) 燃烧证明
Proof of Burn

C) 权益证明（PoS）
Proof of Stake (PoS)

D) 工作量证明（PoW）
Proof of Work (PoW)

14 / 40

哪一种共识算法**最不**节能？

Which consensus algorithm is the **least** energy efficient?

A) 股份授权证明机制（DPoS）
Delegated Proof of Stake (DPoS)
B) 权威证明（PoA）
Proof of Authority (PoA)
C) 空间证明（PoSpace）
Proof of Space (PoSpace)
D) 工作量证明（PoW）
Proof of Work (PoW)

15 / 40

使用证明已用时间证明（PoET）这种共识算法而不是工作量证明（PoW）有什么优点？

What is an advantage of using the consensus algorithm Proof of Elapsed Time (PoET) instead of Proof of Work (PoW)?

A) PoET通常比PoW更容易被用于非许可链，因为PoET的摇号系统用来选择节点比较安全。
PoET can often be used in a permissionless blockchain more easily than PoW, because PoET's lottery system for node selection is secure.
B) PoET的交易成本通常低于PoW，因为其所需的硬件比PoW更为通用。
PoET has generally lower transaction costs than PoW, because the hardware needed is more generic than the hardware needed for PoW.
C) PoET比PoW安全得多，因为PoET通过为交易加上时间戳来支持可信执行环境（TEE）。
PoET is much more secure than PoW, because PoET supports the trusted execution environment (TEE) by time-stamping the transactions.
D) PoET通常比PoW更快，因为与PoW相比，竞争验证的节点更少，原因是PoET随机选择节点。
PoET is usually faster than PoW, because fewer nodes compete for validation than in PoW, since PoET randomly selects the nodes.

16 / 40

攻击者试图破坏区块链的交易历史，以便能够使用通证或加密货币两次。

攻击者**最**可能做的事情是什么？

An attacker tries to corrupt the transaction history of a blockchain to be able to spend a token or a cryptocurrency twice.

What is the **most** likely thing this attacker did?

A) 攻击者更改了节点上的交易并在网络中传播。
The attacker changed the transaction on his node and propagated it in the network.
B) 攻击者编辑了智能合约，恢复了投资者的加密货币。
The attacker edited the smart contract and recovered investor's cryptocurrency.
C) 攻击者控制了网络超过51%的计算能力。
The attacker gained control of more than 51% of the network's computing power.
D) 攻击者对网络进行了硬分叉并创建了新的区块链网络。
The attacker hard-forked the network and created a new blockchain network.

17 / 40

区块链网络容易受到51%攻击。

哪种网络**最容易**诱发黑客攻击并破坏网络?

Blockchain networks are vulnerable to 51% attacks.

Which network would incentivize hackers **most** to break the network?

A) 比特币
Bitcoin
B) Fabric
Fabric
C) 瑞波币
Ripple

18 / 40

区块链社群所面临的最大威胁之一是对微小差异的自恋情节。

这种对微小差异的自恋情节会产生什么结果?

One of the greatest threats to the blockchain community is the narcissism of small differences.

What is the result of this narcissism of small differences?

A) 一个社群在小差异上取笑另一个社群，将导致更大的合作。
One community group makes fun of another community group over small differences, resulting in greater collaboration.
B) 社群关心并努力解决外部群体无法察觉的微小差异。
The community cares about and works to resolve small differences that cannot be perceived by outside groups.
C) 社群已经开发了许多类似的项目，这些项目因微小的差异而互相争斗。
The community has developed many similar projects and these fight with one another over small differences.
D) 社群变得更加紧密，并以协作的方式合作解决共同的问题。
The community has grown closer and works together in a collaborative fashion to solve common problems.

欺诈者如何使用庞氏骗局？

How do fraudsters use a Ponzi scheme?

A) 欺诈者说服受害人为以后收到更值钱的东西而付钱。
A fraudster convinces a victim to pay for receiving something of greater value later on.
B) 欺诈者找到投资者，然后抛售投资者的通证，使市场崩溃。
A fraudster finds investors, then dumps the tokens of the investors to crash the market.
C) 欺诈者使用后续投资者的资金向初始投资者支付股息。
A fraudster pays dividends to initial investors using the funds of subsequent investors.
D) 欺诈者窃取信用卡并用其购买金钱、商品或财产。
A fraudster steals credit cards and uses them to buy money, goods or property.

区块链网络的哪个特征同时起到保护作用？

Which characteristic of a blockchain network is also its protection?

A) 完全独立节点的数量越多，破坏区块链中数据的难度越大。
The greater the number of full independent nodes, the harder it is to compromise the data in the blockchain.
B) 区块链中矿工的数量越少，保护网络安全的动力就越高。
The lower the number of miners in the blockchain, the higher the incentive is for securing the network.
C) 区块链的控制权越集中，保护数据安全和避免欺诈的难度越大。
The more centralized the control of the blockchain is, the harder it is to secure the data and avoid fraud.
D) 工作量证明（PoW）算法越复杂，保护网络安全的奖励越多。
The more complicated the Proof of Work (PoW) algorithm is, the more rewarding it is to secure the network.

如何在区块链中保护信息安全？

How can information be secured in a blockchain?

A) 利用封闭的对等（P2P）网络，跨平台共享信息
By using a closed peer-to-peer (P2P) network, sharing information across platforms
B) 通过网络进行矿工间的加密货币分配
By using a distribution of cryptocurrencies over miners through the network
C) 使用由公钥和私钥组成的非对称加密技术
By using asymmetric cryptography, consisting of a public and private key
D) 利用分布式账本技术（DLT），在源头记录交易。
By using distributed ledger technology (DLT), which records transactions at the source

区块链以何种方式运用公众见证?

In what way do blockchains use a public witness?

A) 数字法院或图书馆充当公众见证，存储信息以供参考。
A digital courthouse or library acts as a public witness to store information to reference.
B) 区块链网络上的节点证明信息的准确性和真实性。
A node on a blockchain network attests to the accuracy and truthfulness of information.
C) 一个人通过一个公共网络发送一个交易，作为公众见证可以获得奖励。
A person sends a transaction over a public network to earn rewards as a public witness.
D) 可以选择一个首选节点来证明信息的准确性和真实性。
A preferred node can be elected to attest to the accuracy and truthfulness of information.

区块链实现自我主权身份。

区块链如何做到这一点?

Blockchain enables self-sovereign identity.

How does blockchain do this?

A) 它使中心化的第三方能够提供易于使用和有效的身份信息。
It enables centralized third parties to offer easy-to-use and valid identity information.
B) 它使每个人都可以完全控制自己的金钱、财产和身份。
It enables each person to have exclusive control of their money, property and identity.
C) 它使政府能够轻松地颁发高级数字证书身份。
It enables governments to effortlessly issue identities with advanced digital certificates.
D) 它仅允许互联网公司提供世界一流的安全个人身份存储库。
It enables only internet companies to offer world-class secure personal identity repositories.

公有链鼓励用户挖掘区块并保护网络安全。

这是什么激励?

Public blockchains give an incentive to encourage users to mine blocks and secure the network.

What incentive is this?

A) 公有链允许用户创造通证并在二级市场上销售。
Public blockchains allow users to create tokens to sell on secondary markets.
B) 公有链不提供奖励，因为它们是开源的。
Public blockchains do not offer rewards, because they are open source.
C) 公有链为运行挖矿节点提供现金奖励。
Public blockchains offer cash rewards for running mining nodes.
D) 公有链以加密货币的形式提供挖矿奖励。
Public blockchains offer rewards for mining in the form of cryptocurrency.

一个组织机构想要开发基于区块链技术的智能合约。该组织机构不希望让员工承担维护区块链安全的负担。

什么样的区块链技术**最**适合该组织?

An organization wants to develop smart contracts, based on blockchain technology. The organization does not wish to burden employees with maintaining the security of the blockchain.

What blockchain technology fits the organization **best**?

A) 混合链
A hybrid blockchain
B) 私有链
A private blockchain
C) 公有链
A public blockchain

超级账本网络的**关键**特点是什么?

What is a **key** characteristic of the Hyperledger network?

A) 它是一个公共区块链网络,也是自2009年以来最古老的网络之一。
It is a public blockchain network and one of the oldest networks, existing since 2009.
B) 它是私有、开源的,可运行个人的分布式账本技术(DLT)。
It is private, open sourced and can run everyone's own distributed ledger technology (DLT).
C) 它利用加密货币作为奖励机制,从而提高网络安全性。
It utilizes cryptocurrency as a reward mechanism, which makes the network more secure.
D) 它利用权益证明(PoS)共识算法作为主要安全措施。
It utilizes the Proof of Stake (PoS) consensus algorithm as its main security measure.

智能合约的**最佳**使用案例是什么?

What is the **best** use case for smart contracts?

A) 使用人工智能(AI)将具有法律约束力的合同数字化和自动化
Digitalize and automate legally binding contracts using artificial intelligence (AI)
B) 使用加密货币在法律体系中强制执行合约
Enforce the execution of contracts in the legal system using cryptocurrencies
C) 通过保险合约中的预定行为或事件确保自动付款
Ensure automatic payments by predetermined actions or events in insurance contracts
D) 将最著名的智能合约平台,即比特币区块链扩展到司法制度
Extend the Bitcoin blockchain, the best-known smart contract platform, to the judicial system

28 / 40

在哪种情况下，智能合约是问题的**最佳**解决方案？

In which scenario is a smart contract the **best** solution to the problem?

A) 一个酒保想通过把加密货币转移到他的钱包里来强迫顾客付饮料费。
A bartender wants to force customers to pay for their drinks by transferring cryptocurrency to his wallet.

B) 一位首席财务官希望她的智能手表在她的合作伙伴进入他们的前门时通知她。
A chief financial officer wants her smart watch to notify her when her partner enters their front door.

C) 一个能源公司希望在价格达到预定费率时自动购买电力。
An energy company wants to automatically buy power when the price reaches a predetermined rate.

D) 一个保险公司希望在专案经理认为最佳的情况下向农民付款。
An insurance company wants to pay out a farmer whenever the case manager feels it is best to do so.

29 / 40

DApp的用途是什么？

What are DApps designed to do?

A) 在独立应用程序的前端使用业务逻辑执行智能合约
Execute smart contracts with the business logic in the front-end of a standalone application

B) 仅管理加密货币，无需用到治理区块链的任何嵌入式投票系统
Manage cryptocurrencies only, without any embedded voting system for governance of the blockchain

C) 在对等网络（P2P）上运行应用程序，将智能合约的运用范围扩展到简单的价值转移以外
Run applications on a peer-to-peer (P2P) network expanding smart contracts beyond simple value transfer

D) 支持在多个公共云提供商上运行的应用程序，避免任何供应商锁定和欺诈
Support applications that run on multiple public cloud providers avoiding any vendor lock-in and fraud

30 / 40

去中心化自治组织(DAO)的作用是什么？

What is the role of a DAO (decentralized autonomous organization)?

A) 通过在商定规则内进行协作和认可的行为来解决委托-代理困境
Address the principal-agent dilemma with collaboration and acceptance of actions within agreed rules

B) 使用公有链将当前的司法系统嵌入受监管的在线智能合约
Embed regulated online smart contracts with the current judicial system, using public blockchains

C) 提供复杂的在线智能合约，无需绑定有形和无形的离线资产
Offer complex online smart contracts without any link to tangible and intangible offline assets

D) 提供一个私有链合约平台，用户可以在该平台上运行其在线应用程序
Provide a private blockchain contract platform on which users can run their online applications

区块链技术如何能够**最好地**帮助保护身份数据安全?

How can blockchain technology **best** help securing identity data?

A) 通过在用户服务器上提供安全数据存储来免除第三方介入
By eliminating third parties through providing secured-data storage at a user's server

B) 将所有健康数据编码并保存在私有、非许可链中
By encoding all the health data and save it on a private and permissionless blockchain

C) 通过使用加密算法保护已在互联网上提交的数据
By protecting data that has been submitted on the internet using a cryptographic algorithm

D) 提供个人数据信息而不披露能够证明其真实性的实际数据
By providing information personal data without disclosing the actual data that proves it

将区块链网络与物联网(IoT)结合的价值是什么?

What is the value of using blockchain networks with Internet of Things (IoT)?

A) 允许区块链用户跟随和访问自动驾驶汽车
Allowing blockchain users to follow self-driving cars and access these cars

B) 使用存储在区块链上的安全身份避免电子欺骗攻击
Avoiding a spoofing attack using the secured identity that is stored on a blockchain

C) 启用可自行编程的软件,可无需人工干预解决问题
Enabling software that programs itself to solve problems without human intervention

D) 使用超级账本Fabric挖矿解决昂贵而复杂的计算
Solving expensive and complex calculations using Hyperledger Fabric mining

区块链技术实现了去中心化市场。

去中心化市场有什么好处?

Blockchain technology has made decentralized marketplaces possible.

What is a benefit of a decentralized marketplace?

A) 它基于开源技术,因此使用时无需任何投资。
It is based on open-source technology, so it can be used without any investment.

B) 它无需付费的许可证就可以经营,因此可以得到更好的管理。
It is not under a paid license to operate and therefore it is managed better.

C) 因使用加密货币,它的成本相对较低,而且非常容易访问。
It is relatively cheap due to the use of cryptocurrency and is very accessible.

D) 由于智能合约,它具有防篡改功能,抗关闭能力,以及可信赖性。
It is tamper-proof, resilient to being shut down and trustworthy due to smart contracts.

区块链如何改善供应链?

How does blockchain improve supply chains?

A) 通过自动创建双方之间的贸易协议
By automatically creating trade agreements between two parties
B) 通过创建安全的集中化市场进行商品交易
By creating safe centralized marketplaces to trade goods on
C) 通过稳定相关国家的本国货币
By stabilizing the national currencies of the countries involved
D) 通过软件系统转移通证化所有权
By transferring tokenized ownership through a software system

新加坡金融管理局（MAS）与区块链公司R3合作。

双方共同取得了什么成就?

The Monetary Authority of Singapore (MAS) and blockchain company R3 partnered together.

What did they achieve together?

A) 创建了智能合约和稳定币
The creation of smart contracts and stable coins
B) 促进了银行间消息传递
The facilitation of interbank transmission of messages
C) 不受时区限制的首次跨行支付
The first interbank payments without limitations of time zones
D) 发布采用加密技术的电汇
The launch of wire transfers using cryptography

什么是法定数字货币?

What is digital fiat currency?

A) 代表一个国家财政储备的货币的数字形式
A digital form of currency, that represents a country's financial reserves
B) 一种创建透明且无国界债务市场的电子货币
An e-currency, that creates a transparent and borderless debt market
C) 一种无需银行账户即可进行交易的在线系统
An online system, that enables making transactions without a bank account

37 / 40

区块链技术如何使保险业受益？

How does blockchain technology benefit the insurance industry?

A) 避免了国家主管部门的合规性要求，从而减少了开销
    By avoiding compliance requirements of national authorities, which reduces overhead

B) 确保了数据的准确性和实现小额保险自动化，从而降低了成本
    By ensuring accuracy of data and automating micro insurances, which reduces costs

C) 引入了客户支付灵活的保费，从而增加利润
    By introducing flexible premiums to be paid by customers, which increases profits

D) 设置了数字付款方式，从而简化了理赔
    By setting up a digital mode of payment, which simplifies claims settlement

38 / 40

区块链技术如何帮助保护知识产权(IP)？

How does blockchain technology help to protect intellectual property rights (IP)?

A) 它允许用户将IP交易包括在智能合约中。
    It allows a user to include IP transactions in smart contracts.

B) 它允许用户记录事件并建立时间线。
    It allows a user to record an event and establish the timeline.

C) 它允许用户记录软件包的创建。
    It allows a user to record the creation of software packages.

D) 它允许用户发送交易和获得IP所有权。
    It allows a user to send a transaction and receive IP ownership.

39 / 40

哪一项属于政府积极促进区块链应用的案例？

What is an example of how a government is actively promoting the use of blockchain?

A) 中国创建了一个监管沙盒，允许他们密切监控区块链挖矿中的实验，并创建各自的加密货币。
    China has created a regulatory sandbox that allows them to closely monitor the experiments in blockchain mining and create their own cryptocurrency.

B) 爱沙尼亚提供电子居留权（e-Residency）软件，世界上任何有兴趣在网上和欧盟内部经营企业的人都可以使用。
    Estonia offers e-Residency software, which is available to anyone in the world interested in operating a business online and from within the European Union.

C) 新加坡金融管理局(MAS)正在使用分布式账本技术(DLT)为银行间支付创造中央银行数字货币。
    Singapore's Monetary Authority (MAS) is creating central bank digital money for payments between banks using distributed ledger technology (DLT).

为什么将区块链描述为可增加互联网信任度的技术?

Why is blockchain described as the technology that adds a layer of trust to the internet?

A) 区块链允许个人和团体一起工作，而不必相互信任或建立权威。
It allows individuals and groups to work together without having to trust each other or establish authority.

B) 区块链创建两方或多方之间的虚拟专用网络（VPN）隧道，以进行在线转账。
It creates a dedicated virtual private network (VPN) tunnel between two or more parties to carry out online fund transfers.

C) 区块链提供了一种机制，使政府可以创建自己的法定数字货币来代替实物货币。
It provides mechanism for the government to create their own digital fiat currency as a replacement of physical currency.

D) 区块链提供了多因素身份验证，可以安全地创建和更新加密货币交易记录。
It provides multifactor authentication to create and update records of cryptocurrency transactions securely.

答案解析

1 / 40
哪一项是公有链的优点?

What is an advantage of a public blockchain?

A) 公有链不使用无利害关系的第三方保护区块安全,因为所有参与者都具有既得利益。
It does not use disinterested third parties to secure blocks, as all participants have a vested interest.
B) 公有链具有更强的抵御欺诈能力,因为它使用联盟节点来对抗欺诈。
It is more resilient against fraud, because it uses federated nodes to combat fraud.
C) 公有链对全世界所有人开放,无需许可和授权要求。
It is open to everyone in the world without permission and licensing requirements.
D) 公有链网络由营利性公司构建,网络的正常运行有所保障。
Its networks are built by for-profit companies and the working of the network is guaranteed.

A) 错误。以上说的是许可链节点的优点。许可链节点是指运用某些而非全部区块链技术的私有网络。大多数都未包含挖矿,也没有原生加密货币。因此,没有无利害关系的第三方。区块和交易由已知参与者处理。
Incorrect. This is an advantage of permissioned blockchain nodes. Permissioned blockchain nodes are private networks that use some blockchain technology but not all. Most do not incorporate mining and do not have a native cryptocurrency. Thus, there are no disinterested third parties. The blocks and transactions are processed by known participants.
B) 错误。联盟节点可以存在于公共和私有区块链中。公共区块链也可以在没有联盟的情况下存在。联盟是指系统,确切地说是系统的用户,选择节点处理交易时的情况。
Incorrect. Federated nodes can exist in both public and private blockchains. Public blockchains can also exist without federation. Federation is when the system, or rather the user of a system, elects nodes to process transactions.
C) 正确。这是公有链的一个优势。公有链向世界上任何一个参与网络功能的人开放,只是受到接入互联网、硬件和电力的限制。(文献:A,第1.1章)
Correct. This is an advantage of public blockchains. Public blockchains are open to anyone in the world to participate in the functions of the network, only limited by their access to the internet, hardware, and electricity. (Literature: A, Chapter 1.1)
D) 错误。根据定义,公有链持有开放式许可证(例如Apache或MIT许可证)。不存在门控机制,无需向任何人征求许可,也没有许可费。
Incorrect. Public blockchains are by definition held in an open license such as the Apache or MIT license. There are no gating mechanisms, no one to ask permission and no licensing fee.

什么是区块链?

What is a blockchain?

A) 一种集中式数据库，存储着所有节点上所有交易记录的子集。
A centralized database that holds a subset of all transactions on all nodes.

B) 一种客户-服务器数据库，数据同时存在于有限数量的节点中。
A client-server database existing on a limited number of nodes at the same time.

C) 一种将所有的交易记录都存储在网络上的分布式数据库。
A distributed database with a record of all transactions on the network.

D) 一种独立运行数据库，由多个节点存储着所有的历史交易记录。
A standalone database with history of all transactions on various nodes.

) 错误。区块链是一种去中心化的对等（P2P）分布式数据库，每个节点都包含所有交易的记录。
Incorrect. Blockchain is a decentralized, peer-to-peer (P2P) distributed database where every node holds record of all transactions.

B) 错误。区块链由P2P分布式数据库组成。
Incorrect. Blockchain consists of P2P distributed databases.

C) 正确。区块链是一种带时间戳的P2P分布式数据库，存储了网络上发生的所有交易的记录。 （文献：A，第1.1章)
Correct. It is a P2P distributed time-stamped database that holds a record of all transactions that have ever occurred on the network. (Literature: A, Chapter 1.1)

D) 错误。区块链是具有所有交易历史记录的去中心化P2P分布式数据库。
Incorrect. Blockchain is a decentralized, P2P distributed database with history of all transactions.

区块链网络中轻节点的功能是什么?

What is the function of a lightweight node within a blockchain network?

A) 轻节点存储网络上每笔交易的完整历史记录。
It stores a complete history of every transaction on the network.

B) 轻节点为区块链网络的用户存储购买的加密货币。
It stores purchased cryptocurrency for users of a blockchain network.

C) 轻节点通过借用全节点的工作来验证交易。
It verifies transactions by piggybacking on the work of full nodes.

A) 错误。节点不一定存储网络上每笔交易的完整历史记录。这仅适用于全节点。
Incorrect. A node does not necessarily store a complete history of every transaction on the network. That is only true for a full node.

B) 错误。节点本身并不存储加密货币，但它存储包含所有交易记录的区块。
Incorrect. A node does not store cryptocurrency itself, but it stores blocks that contain a record of all transactions.

C) 正确。轻节点通过借用全节点的工作来验证交易。 （文献：A，第1.1章)
Correct. Lightweight nodes verify transactions by piggybacking on the work of full nodes. (Literature: A, Chapter 1.1)

哪一项**不属于**节点的类别?

What is **not** a classification for a node?

A) 全节点
Full node
B) 轻节点
Lightweight node
C) 默克尔节点
Merkle node
D) 矿工节点
Miner node

A) 错误。全节点需要所有新的交易记录。它们保留所有区块头。区块头能够识别一个唯一的区块并包含上一个区块的哈希。所有这些数据全部累计起来,会占用大量空间。
Incorrect. Full nodes need all new transaction records. They keep all block headers. Block headers identify a unique block and contain a hash of the previous block. All this data adds up and takes up a lot of room.

B) 错误。轻节点通过借用全节点的工作来验证交易。轻节点仅下载所有区块头,然后利用称为简单支付验证(SPV)的系统检查交易。
Incorrect. Lightweight nodes verify transactions by piggybacking on the work of full nodes. They only download the headers of all blocks and then check transactions utilizing a system called simplified payment verification (SPV).

C) 正确。默尔克树根不属于节点的类别。它是一个哈希,允许混合链在网络受到攻击时恢复至最后一个已知的有效区块。(文献:A,第1.1章)
Correct. Merkle tree root is not a node classification. It is a hash that allows a hybrid blockchain to restore itself to its last known valid block in case its network is attacked.
(Literature: A, Chapter 1.1)

D) 错误。矿工是一种向新区块添加交易的节点。矿工通过相互竞争,并解决复杂的数学问题后,赢得新建一个完整区块的权利。每个矿工将答案写入区块头,如果正确,则会奖励加密货币。
Incorrect. A miner is a type of node that is adding transactions to new blocks. Miners compete to win the right to create a new complete block by solving a complex mathematical problem. Each miner will write their answer in the block header and if they are correct, they are then rewarded with cryptocurrency.

一种无记名票据可通过区块链网络在两方之间转移价值。

以上说的是哪一种票据？

A bearer instrument used to transfer value between two parties over a blockchain network.

What is this instrument?

A) DApp
A DApp
B) 哈希
A hash
C) 节点
A node
D) 通证
A token

A) 错误。DApps是指在对等网络（P2P）而非单个系统上运行的应用程序。DApps是由智能合约构建，但是使用其他服务（例如安全消息），并且通常允许无限数量的参与者在给定规则集中地进行交互。
Incorrect. DApps are applications that run on a peer-to-peer (P2P) network instead of a single system. DApps are built with smart contracts but use other services such as secure messaging and often allow an unlimited number of participants to interact within a given rule set.

B) 错误。哈希函数用于保护交易区块中所有数据的安全。哈希是一个数学过程的输出，该过程创建一串固定长度的数字和字母。
Incorrect. A hash function is used to secure all the data in a block of transactions. A hash is the output of this mathematical process that creates a string of numbers and letters of a fixed size.

C) 错误。节点是连接到区块链网络的计算机。节点运行网络软件，通过跨网络将信息传输到其他节点，保持网络健康。
Incorrect. A node is a computer that is connected to a blockchain network. It runs the software for the network and keeps the network healthy by transferring information across the network to other nodes.

D) 正确。通证是一种无记名票据，可通过区块链网络在两方之间转移价值。（文献：A，第1.1章）
Correct. A token is a bearer instrument used to transfer value between two parties over a blockchain network. (Literature: A, Chapter 1.1)

公有链的**关键**特点是什么?

What is a **key** characteristic of a public blockchain?

A) 允许用户选择节点处理交易
   Allowing a user to elect nodes to process transactions
B) 允许任何人参与区块链网络
   Allowing anyone to participate in the blockchain network
C) 允许控制参与的主体以及参与的级别
   Allowing control over who can participate and at what level
D) 仅允许可信方操作其区块链
   Allowing only trusted parties to operate their blockchain

A) 错误。联盟链节点可以同时存在于公有链和私有链中。联盟是指系统,确切地说是系统的用户,推选节点处理交易时的情况。
   Incorrect. Federated blockchain nodes can exist in both public blockchains and private blockchains. Federation is when the system, or rather the user of a system, elects nodes to process transactions.
B) 正确。公有链允许任何人参与到网络中,只要可以接入互联网、硬件和电力。(文献:A,第1.1章)
   Correct. Public blockchains allow anyone to participate in the network as long as they have access to the internet, hardware and electricity. (Literature: A, Chapter 1.1)
C) 错误。混合链控制参与的主体以及允许每个节点操作的参与级别。
   Incorrect. Hybrid blockchains control who can participate and at what level of participation each node is allowed to operate.
D) 错误。私有链仅允许可信方操作其区块链。
   Incorrect. Private blockchains only allow trusted parties to operate their blockchain.

哪一项属于密码学在区块链的应用案例?

What is an example of the use of cryptography in a blockchain?

A) 使用私钥访问私有链或混合链
Accessing private or hybrid blockchains by using a private key
B) 创建加密货币作为挖矿节点的奖励
Creating cryptocurrency as a reward for mining nodes
C) 保护区块链免受损坏节点的51%攻击。
Keeping blockchains secure from 51% attacks by corrupt nodes
D) 确保接受者之间加密货币的安全转移
Securing transfers of cryptocurrency between recipients

A) 错误。即使使用私钥和公钥,密码学也不是用来访问混合链或私有链。
Incorrect. Cryptography is not used to enter hybrid or private blockchains, even if they use private and public keys.
B) 错误。一些区块链网络用加密货币奖励挖矿节点。然而,这不是密码学所做的。
Incorrect. Some blockchain networks reward mining nodes with cryptocurrency. However, this is not what cryptography does.
C) 错误。密码学有助于保护区块链,但不一定能免受51%攻击。
Incorrect. Cryptography helps secure blockchains, but not necessarily against a 51% attack.
D) 正确。区块链技术运用的非对称加密允许发送者将加密货币转给接收者,其他人无法窃取。 (文献:A,第2.1章)
Correct. The asymmetric encryption blockchain technology uses, allows a sender to transfer cryptocurrency to the recipient without someone else being able to steal it. (Literature: A, Chapter 2.1)

区块链如何利用私钥和公钥加密?

How do blockchains use private and public-key cryptography?

A) 非对称加密允许发送者将加密货币转移至公钥。然后，接收者可用各自的私钥访问资金并将资金存入钱包。
Asymmetric encryption allows a sender to transfer cryptocurrency to a public key. The recipient can then access these funds with their private key and hold it in their wallet.

B) 在公钥加密中，一个密钥用于对交易进行加密和解密。发送方使用此密钥发送加密货币，而接收方的钱包在解密后保存加密货币。
In public-key cryptography, one key is used to encrypt and decrypt transaction. The sender uses this key to send cryptocurrency and the recipient's wallet holds it after decryption.

C) 对称加密允许发送者向另一个用户传输加密货币。然后，当发送方授予对其私钥的访问权时，接收方可以访问其资金。
Symmetric encryption allows a sender to transfer cryptocurrency to another user. The recipient can then access their funds when the sender grants access to their private key.

D) 区块链中的算法将私钥和公钥加密并存储到所有用户的钱包中。然后，用户通过二十位口令密钥访问其资金。
The algorithm in the blockchain encrypts and stores private and public keys to all user's wallets. The user then accesses their funds through their twenty-word passphrase key.

A) 正确。非对称加密允许任何人使用收件人的公钥加密消息，而加密的消息只能使用收件人的私钥读取。非对称加密允许发送方向接收方传送加密货币，而其他人无法窃取。这使得他们无需会面或交换信息就能做到这一点。只要发送方拥有接收方的公钥，就可以向其发送加密货币。(文献:A，第2章)
Correct. Asymmetric cryptography allows anyone to encrypt a message using the recipient's public key, whilst the encrypted message can only be read using the recipient's private key. Asymmetric encryption allows a sender to transfer cryptocurrency to the recipient without someone else being able to steal it. It allows them to do this without having met or exchanged information. As long as the sender has the public key of the recipient, they can send them cryptocurrency. (Literature: A, Chapter 2)

B) 错误。公钥加密使用两个密钥，一个公钥和一个私钥。希望向新地址发送加密货币的用户将使用他们的私钥在交易中签名，然后将其发送到公钥，即地址。然后，接收人将使用他们的私人密钥访问资金。
Incorrect. Public-key cryptography uses two keys, a public and a private key. Users that wish to send cryptocurrency to a new address would sign the transaction with their private key and then send it to the public key, known as the address. The recipient would then use their private keys to access the funds.

C) 错误。区块链不使用这种类型的加密，因为这种类型的加密只有一个密钥，用户必须碰面交换信息。
Incorrect. Blockchains do not use this type of encryption as there is only one key with this type of encryption and the users will have to meet to exchange information.

D) 错误。区块链只有加密货币的公开地址。私钥由所有者安全持有。如果私钥丢失，可以使用密码短语来恢复私钥。
Incorrect. Blockchains only have the public address for cryptocurrency. The private key is held securely by the owner. Passphrases can be used to recover private keys if they are lost.

混合链网络如何对抗51%攻击？

How do hybrid blockchain networks combat 51% attacks?

A) 通过一个中央控制器，确保网络中每个节点的安全
Through a central controller ensuring the security of each node in the network

B) 通过一个工作量证明（PoW）算法，允许矿工保护网络安全
Through a Proof of Work (PoW) algorithm, which allows miners to secure the network

C) 通过激励，矿工通过确保网络安全而获得货币
Through incentivization, where miners receive currency for securing the network

D) 通过默克尔树根，允许网络将自身还原到其最后一个有效区块
Through Merkle tree roots, that allow the network to restore itself to its last valid block

A) 错误。默克尔树根是一种保护混合网络的方法。混合链不需要中央控制器。
Incorrect. Merkle Tree roots are a way to secure hybrid networks. Hybrid blockchains do not go through a central controller.

B) 错误。加密是任何类型区块链的通用安全功能，并不特定于混合网络。
Incorrect. Encryption is a generic security functionality of any kind of blockchain and is not specific to hybrid networks.

C) 错误。激励机制对公有链有效，但对混合链无效。
Incorrect. An incentivization mechanism works well for public blockchains, but not for hybrid blockchains.

D) 正确。混合链网络通过默克尔树根的哈希值进行安全保护，允许网络在损坏的情况下将自身恢复到其最后已知的有效区块。（文献：A，第1.1章）
Correct. Hybrid blockchain networks are secured through Merkle tree root hashes, which allow the network to restore itself to its last known valid block in case of corruption. (Literature: A, Chapter 1.1)

区块链如何像账本一样发挥作用?

How do blockchains function like ledgers?

A) 区块链保留了网络上发生的所有交易的记录。
   They hold a record of all transactions that have ever occurred on a network.
B) 区块链将大量交易数据保存为一个中央数据库。
   They hold vast amounts of transaction data as a centralized database.
C) 区块链定期更新区块链中每个钱包的所有余额。
   They periodically update all balances of each wallet to the blockchain.

A) 正确。区块链是分布广泛的公共账户，任何人都可以查看加密货币的持有人和币种以及该币的全部历史。可以找到每笔交易以及交易涉及的各方。（文献：A，第2.1章）
   Correct. Blockchains are widely distributed public accounts that let anyone see who has what cryptocurrency and the full history of that coin over time. Every transaction can be found as well as the parties involved in these transactions. (Literature: A, Chapter 2.1)
B) 错误。区块链是广泛的分布式账本，只储存数量有限的交易数据。因为它们是分布式的，所以大小是受限制的，共享和协调大量数据是不现实的。
   Incorrect. Blockchain are widely distributed ledgers that hold a limited amount of transaction data. The size limit is restricted because they are distributed, and it is impractical to share and reconcile vast quantities of data.
C) 错误。钱包不保留私人账本。钱包从区块链收集余额数据。
   Incorrect. Wallets do not keep a private ledger. They pull in balance data from a blockchain.

区块链网络中矿工的任务是什么?

What is the task of miners in a blockchain network?

A) 矿工作为单一的第三方来收集记录，并通过矿工权威当局向网络提供信任。
Miners act as a single third party to aggregate records and provide trust in the network by the miners' authority.

B) 矿工是允许访问区块链的计算机，确保损坏节点的数量保持较低水平。
Miners are computers that allow access to the blockchain, ensuring the number of corrupt nodes will stay low.

C) 矿工是通过计算正确的随机数促成交易而竞争奖励的节点。
Miners are nodes that compete for a reward by calculating the correct nonce to make a transaction possible.

D) 矿工决定应遵守的共识规则，并在这些规则被打破时进行干预。
Miners determine the consensus rules that should be followed and interfere when these rules are broken.

A) 错误。中本聪希望通过引入区块链技术来避免单一的第三方。
Incorrect. Needing a single third party was exactly what Satoshi wanted to avoid by introducing blockchain technology.

B) 错误。矿工不负责区块链的准入访问。
Incorrect. Miners are not responsible for access to the blockchain.

C) 正确。矿工们通过努力计算随机数来竞争获得奖赏。（文献：A，第1.1章）
Correct. Miners compete for a reward by trying to calculate the nonce. (Literature: A, Chapter 1.1)

D) 错误。矿工不决定区块链中的规则。矿工在提前设定好规则的场景下作业。
Incorrect. Miners do not determine the rules in blockchain. Miners operate in the playing field determined by the rules.

哪一项描述**仅**符合工作量证明（PoW）共识算法？

Which description fits **only** the Proof of Work (PoW) consensus algorithm?

A) 一种协作共识算法，由被授权的账户执行验证。
A collaborative consensus algorithm, where approved accounts do the validation.

B) 一种由农民推动的协作共识算法，他们提供计算机剩余的内存，使交易成为可能。
A collaborative consensus algorithm that is facilitated by farmers, who offer leftover memory of their computer to make transactions possible.

C) 一种共识算法，对整个交易流程进行验证，包括正确性以及交易顺序。
A consensus algorithm, where the validation is done for the entire transaction flow, including not only the correctness, but also the sequence of transactions.

D) 一种低成本的快速算法，节点需要存入加密货币以担保交易进行。
A low-cost and fast algorithm, where a node needs to deposit cryptocurrency to guarantee the transaction.

E) 一种非竞争性共识算法，验证由选定节点执行，而选定节点将加密货币发送到一个地址，而从这个地址加密货币无法被收回。
A noncompetitive consensus algorithm, where validation is done by elected nodes, which send cryptocurrency to an address, from which it cannot be retrieved.

F) 一种涉及协同验证的算法，协同验证由共识之外选择的验证者执行。
An algorithm that involves collaborative validation, performed by validators, which are chosen outside of the consensus.

G) 一种算法，可在可信执行环境中工作，并证明交易发生的时间。
An algorithm that works in a trusted execution environment and proves the time when the transaction has taken place.

H) 一种高强度且昂贵的竞争性算法，其中区块链上的每个挖矿节点都在相互竞争从而确保其获得区块。
An intensive and expensive, competitive algorithm where each mining node on the blockchain is competing to secure blocks.

A) 错误。以上是权威证明（PoA）的定义。
Incorrect. This is the definition of Proof of Authority (PoA).

B) 错误。以上是容量证明（PoC）和空间证明（PoSpace）的定义。
Incorrect. This is the definition of Proof of Capacity (PoC) and Proof of Space (PoSpace).

C) 错误。这就是超级账本Fabric的定义。
Incorrect. This is the definition of Hyperledger Fabric.

D) 错误。以上是权益证明（PoS）的定义。
Incorrect. This is the definition of Proof of Stake (PoS).

E) 错误。以上是燃烧证明的定义。
Incorrect. This is the definition of Proof of Burn.

F) 错误。以上是股份授权证明机制（DPoS）的定义。
Incorrect. This is the definition of Delegated Proof of Stake (DPoS).

G) 错误。以上是所用时间证明（PoET）的定义。
Incorrect. This is the definition of Proof of Elapsed Time (PoET).

H) 正确。以上正是PoW的定义。（文献：A，第3.1章）
Correct. This is the definition of PoW. (Literature: A, Chapter 3.1)

13 / 40

一种竞争性共识算法因区块链难以满足交易速度要求而开发。

以上说的是哪一种共识算法？

A competitive consensus algorithm that was developed because blockchains had difficulty meeting the transaction speed demands.

Which consensus algorithm is this?

A) 股份授权证明机制（DPoS）
Delegated Proof of Stake (DPoS)

B) 燃烧证明
Proof of Burn

C) 权益证明（PoS）
Proof of Stake (PoS)

D) 工作量证明（PoW）
Proof of Work (PoW)

A) 错误。DPoS是一项协作工作。验证交易的节点将获得同等的奖励。利益相关者为网络选举出验证交易和创建区块的见证人。
Incorrect. DPoS is a collaborative effort. Nodes that are validating transactions are rewarded equally. Stakeholders elect witnesses who will validate transactions and create blocks for the network.

B) 错误。燃烧证明是一种非竞争性共识算法。
Incorrect. Proof of Burn is a noncompetitive consensus algorithm.

C) 正确。PoS是一种竞争性共识算法。由于区块链难以满足交易速度要求，所以它被创建为PoW的替代品，PoS节点不挖掘加密货币。用户可以将区块链中的一些加密货币存入定金。这笔定金允许用户对其行为"下注"：自己将会秉持诚信原则并遵循共识系统的规则进行交易处理。如果用户失信，将没收其加密货币。（文献：A，第3.2章）
Correct. PoS is a competitive consensus algorithm. It was created as an alternative to the PoW because blockchains had difficulty meeting the transaction speed demands. PoS nodes do not mine cryptocurrency. Users can put some of their cryptocurrency, from a blockchain, in a retainer. This retainer allows the user to "stake" that they will process transactions honestly and by the rules of the consensus system. If the user fails to do so, they will forfeit their cryptocurrency. (Literature: A, Chapter 3.2)

D) 错误。PoW是一种竞争性共识算法，区块链上的每个挖矿节点都在互相竞争从而确保其获得区块。它允许任何人参与任何级别的系统创建和维护，但竞争非常激烈。若节点希望具有竞争力并获得加密货币奖励，则需要运行专用设备。PoS的创建是对PoW的替代，以满足较高的交易速度要求。
Incorrect. PoW is a competitive consensus algorithm where each mining node on the blockchain is competing to secure blocks. It allows anyone to participate at any level in the creation and maintenance of the system but is very competitive. Nodes that hope to be competitive and be rewarded with cryptocurrency will need to operate specialized equipment. PoS was created as an alternative to the PoW that required high transaction speed demands.

哪一种共识算法**最不**节能?

Which consensus algorithm is the **least** energy efficient?

A) 股份授权证明机制（DPoS）
Delegated Proof of Stake (DPoS)

B) 权威证明（PoA）
Proof of Authority (PoA)

C) 空间证明（PoSpace）
Proof of Space (PoSpace)

D) 工作量证明（PoW）
Proof of Work (PoW)

A) 错误。DPoS是一项协作工作，在该共识系统中，验证交易的节点将获得同等的奖励。它比较节能，挖矿时不耗电。
Incorrect. DPoS is a collaborative effort, and nodes that are validating transactions are rewarded equally in this consensus system. It is energy efficient and does not burn electricity when mining.

B) 错误。PoA区块链具有协作共识算法。在此系统中，交易和区块由被授权的账户执行验证。验证人节点运行共识软件，允许其将交易输入区块。由于验证人数量有限，所以非常节能。
Incorrect. PoA blockchains have a collaborative consensus algorithm. In this system, transactions and blocks are validated by approved accounts. The validator nodes run consensus software, allowing them to put transactions in blocks. Because of the limited number of validators, it is energy efficient.

C) 错误。PoSpace利用剩余内存，而非处理能力，来互相竞争来保护区块链安全。PoSpace区块链可能是比其他区块链更公平、更节能的选择。它们可用于构建应用程序和转移价值。
Incorrect. Instead of using processing power to compete to secure the blockchain, it uses leftover memory. PoSpace blockchains may be a fairer and greener alternative to other blockchains. They can be used to build applications and transfer value.

D) 正确。从设计上讲，这种算法能耗大且成本高。获取比特币的费用和难度是通证经济学需要特意考虑的一部分。就像开采黄金一样，它既不便宜也不容易开采，比特币的获取难度和稀缺被认为是推动资产价值的一部分因素。(文献:A，第3.1章)
Correct. This algorithm is, by design, energy intensive and expensive. The expense and difficulty of obtaining bitcoins was an intentional part of the token economics. Much like mining gold, it is not cheap nor easy to mine, and the difficulty and scarcity of bitcoins is thought to drive part of the value of the asset. (Literature: A, Chapter 3.1)

使用证明已用时间证明（PoET）这种共识算法而不是工作量证明（PoW）有什么优点?

What is an advantage of using the consensus algorithm Proof of Elapsed Time (PoET) instead of Proof of Work (PoW)?

A) PoET通常比PoW更容易被用于非许可链，因为PoET的摇号系统用来选择节点比较安全。
PoET can often be used in a permissionless blockchain more easily than PoW, because PoET's lottery system for node selection is secure.

B) PoET的交易成本通常低于PoW，因为其所需的硬件比PoW更为通用。
PoET has generally lower transaction costs than PoW, because the hardware needed is more generic than the hardware needed for PoW.

C) PoET比PoW安全得多，因为PoET通过为交易加上时间戳来支持可信执行环境（TEE）。
PoET is much more secure than PoW, because PoET supports the trusted execution environment (TEE) by time-stamping the transactions.

D) PoET通常比PoW更快，因为与PoW相比，竞争验证的节点更少，原因是PoET随机选择节点。
PoET is usually faster than PoW, because fewer nodes compete for validation than in PoW, since PoET randomly selects the nodes.

A) 错误。PoET主要用于许可网络，因为节点需要自我标识。此外，PoET摇号系统存在安全问题。
Incorrect. PoET is used mostly in a permissioned network as the nodes need to identify themselves. Furthermore, PoET's lottery system has security issues.

B) 错误。PoET的交易成本确实较低，但原因并非硬件通用，因为PoET需要用到特定的硬件。
Incorrect. PoET does have lower transaction costs, but the cause is not generic hardware as PoET needs specific hardware.

C) 错误。PoET并不比PoW更安全，即使确实更安全，它也与时间戳无关，因为这种机制仅在节点已知的环境中起作用。
Incorrect. PoET is not more secure than PoW and even if it were, it would have nothing to do with time stamping as this mechanism only works in an environment where the nodes are known.

D) 正确。由于竞争的节点更少，所以PoET的速度更快。（文献：A，第3.1和3.5章）
Correct. The lower number of competing nodes makes PoET faster. (Literature: A, Chapter 3.1 and 3.5)

攻击者试图破坏区块链的交易历史，以便能够使用通证或加密货币两次。

攻击者**最**可能做的事情是什么？

An attacker tries to corrupt the transaction history of a blockchain to be able to spend a token or a cryptocurrency twice.

What is the **most** likely thing this attacker did?

A) 攻击者更改了节点上的交易并在网络中传播。
The attacker changed the transaction on his node and propagated it in the network.

B) 攻击者编辑了智能合约，恢复了投资者的加密货币。
The attacker edited the smart contract and recovered investor's cryptocurrency.

C) 攻击者控制了网络超过51%的计算能力。
The attacker gained control of more than 51% of the network's computing power.

D) 攻击者对网络进行了硬分叉并创建了新的区块链网络。
The attacker hard-forked the network and created a new blockchain network.

A) 错误。其他节点将不接受此交易，因为它将创建比现有链短的侧链。攻击者对一个节点没有足够的挖掘能力，无法获得足够的挖掘能力来创建较长的链。
Incorrect. Other nodes will not accept this transaction because it would create a sidechain that is shorter than the existing chain. The attacker does not have enough mining power with one node to get enough mining power to create a longer chain.

B) 错误。智能合约不太可能被黑客入侵，因为攻击者试图消费两次相同的通证。
Incorrect. It is not likely that a smart contract was hacked, because the attacker tries to spend tokens twice.

C) 正确。这是以太坊经典网络受到攻击时发生的情况。攻击者是一个糟糕的矿工，并回滚了交易历史。攻击者通过控制超过51%的网络计算能力来实现这一点。（文献：A，第10.1章）
Correct. This is what happened in an attack to the Ethereum Classic network. The attacker was a bad miner and rolled back the history of transactions. The attacker did this by gaining control of more than 51% of the network's computing power (51% attack). (Literature: A, Chapter 10.1)

D) 错误。网络未发生硬分叉，因为网络的协议未被大幅修改。
Incorrect. No hard-forking of the network took place, because there was no radical modification to the network's protocol.

区块链网络容易受到51%攻击。

哪种网络**最容易**诱发黑客攻击并破坏网络?

Blockchain networks are vulnerable to 51% attacks.

Which network would incentivize hackers **most** to break the network?

A) 比特币
Bitcoin

B) Fabric
Fabric

C) 瑞波币
Ripple

A) 正确。矿工必须利用他们的计算能力和电力来产生比特币等新的加密货币。如果一个网络变得过于集中,不道德的矿工就可以肆无忌惮地破坏网络。这种特殊类型的漏洞称为51%攻击。51%是为许多区块链创建临界点的数字。如果独立节点较少,则网络将回滚。 (文献:A,第10.1章)
Correct. Miners must use their computing power and electricity to generate new cryptocurrency like bitcoins. If a network becomes too concentrated, criminal miners can corrupt the network with impunity. This particular type of vulnerability is called a 51% attack. 51% is the number that creates a tipping point for many blockchains. If fewer nodes are independent, a network will be rolled back. (Literature: A, Chapter 10.1)

B) 错误。超级账本Fabric没有加密货币。由于没有什么东西可以窃取,黑客们就没有动力去破坏网络。
Incorrect. Hyperledger's Fabric does not have cryptocurrency. With little to steal, hackers are less incentivized to break the network.

C) 错误。比特币不需要用户信任或认识网络上的其他个人,而瑞波币的整个基础架构需要各方在某种程度上相互信任和认识。金融市场主体必须信任其所持有资产的发行者,而节点运营商必须相信,其验证人列表中的其他节点不会共谋,阻止有效交易被确认。由于建立了信任和一致的合作激励机制,这一网络不太可能遭受51%攻击。
Incorrect. Unlike bitcoin, that does not require users to trust or know other individuals on the network, the whole infrastructure of Ripple requires that all parties trust and know one another to some extent. A financial participant must trust the issuers of assets it holds, and a node operator must trust that the other nodes in its validator list will not collude to block valid transactions from being confirmed. Since trust and aligned incentives for cooperation are built in, this network is less likely to suffer a 51% attack.

区块链社群所面临的最大威胁之一是对微小差异的自恋情节。

这种对微小差异的自恋情节会产生什么结果?

One of the greatest threats to the blockchain community is the narcissism of small differences.

What is the result of this narcissism of small differences?

A) 一个社群在小差异上取笑另一个社群，将导致更大的合作。
One community group makes fun of another community group over small differences, resulting in greater collaboration.

B) 社群关心并努力解决外部群体无法察觉的微小差异。
The community cares about and works to resolve small differences that cannot be perceived by outside groups.

C) 社群已经开发了许多类似的项目，这些项目因微小的差异而互相争斗。
The community has developed many similar projects and these fight with one another over small differences.

D) 社群变得更加紧密，并以协作的方式合作解决共同的问题。
The community has grown closer and works together in a collaborative fashion to solve common problems.

A) 错误。各个社群之间没有合作。社群中的裂痕一直延伸到代码，这使得社群一再分裂。
Incorrect. There is no collaboration. The rifts in the communities go all the way down to the code and this has divided the community repeatedly.

B) 错误。社群间更容易互相讥讽和嘲笑，对小事情变得高度敏感。
Incorrect. The communities are more likely to ridicule and mock one another and become hypersensitive to small things.

C) 正确。领域毗邻、关系密切的社群间更容易发生争执。（文献：A，第10.2章）
Correct. Communities with adjoining territories and close relationships are more likely to fight. (Literature: A, Chapter 10.2)

D) 错误。情况正好相反。社群间更容易互相讥讽和嘲笑，而不会加强协作。
Incorrect. The opposite happens. Communities are more likely to ridicule and mock one another than collaborate.

欺诈者如何使用庞氏骗局？

How do fraudsters use a Ponzi scheme?

A) 欺诈者说服受害人为以后收到更值钱的东西而付钱。
A fraudster convinces a victim to pay for receiving something of greater value later on.

B) 欺诈者找到投资者，然后抛售投资者的通证，使市场崩溃。
A fraudster finds investors, then dumps the tokens of the investors to crash the market.

C) 欺诈者使用后续投资者的资金向初始投资者支付股息。
A fraudster pays dividends to initial investors using the funds of subsequent investors.

D) 欺诈者窃取信用卡并用其购买金钱、商品或财产。
A fraudster steals credit cards and uses them to buy money, goods or property.

A) 错误。这是一个预付费的骗局。
Incorrect. This is an advance fee scheme scam.

B) 错误。这是一个操纵市场的骗局
Incorrect. This is a market manipulation scam.

C) 正确。在老派的庞氏骗局中，欺诈者使用后续投资者的资金向初始投资者支付股息。（文献：A，第10.3章）
Correct. In old-school Ponzi schemes, the fraudster pays dividends to initial investors using the funds of subsequent investors. (Literature: A, Chapter 10.3)

D) 错误。以上说的是身份盗用和信用卡诈骗。
Incorrect. This is an identity theft and credit card fraud scam.

区块链网络的哪个特征同时起到保护作用?

Which characteristic of a blockchain network is also its protection?

A) 完全独立节点的数量越多，破坏区块链中数据的难度越大。
The greater the number of full independent nodes, the harder it is to compromise the data in the blockchain.

B) 区块链中矿工的数量越少，保护网络安全的动力就越高。
The lower the number of miners in the blockchain, the higher the incentive is for securing the network.

C) 区块链的控制权越集中，保护数据安全和避免欺诈的难度越大。
The more centralized the control of the blockchain is, the harder it is to secure the data and avoid fraud.

D) 工作量证明（PoW）算法越复杂，保护网络安全的奖励越多。
The more complicated the Proof of Work (PoW) algorithm is, the more rewarding it is to secure the network.

A) 正确。节点高分散性是区块链中的主要安全保障之一。(文献:A，第1.1章)
Correct. Distribution is one of the main security safeguards in a blockchain. (Literature: A, Chapter 1.1)

B) 错误。矿工的动力不是区块链的安全性。
Incorrect. The incentive for miners is not the security of the blockchain.

C) 错误。中央控制器可以通过只与受信任节点工作来使区块链更加安全。
Incorrect. A central controller can create more security of the blockchain by working with only trusted nodes.

D) 错误。PoW的复杂性对区块链的安全性没有贡献。
Incorrect. PoW complexity does not contribute to security of the blockchain.

如何在区块链中保护信息安全？

How can information be secured in a blockchain?

A) 利用封闭的对等（P2P）网络，跨平台共享信息
By using a closed peer-to-peer (P2P) network, sharing information across platforms

B) 通过网络进行矿工间的加密货币分配
By using a distribution of cryptocurrencies over miners through the network

C) 使用由公钥和私钥组成的非对称加密技术
By using asymmetric cryptography, consisting of a public and private key

D) 利用分布式账本技术（DLT），在源头记录交易。
By using distributed ledger technology (DLT), which records transactions at the source

A) 错误。P2P是使用的网络类型，它本身并不是安全措施。
Incorrect. P2P is the type of network being used, it is not a security measure in itself.

B) 错误。加密货币是交换的价值，它并非一种安全工具。
Incorrect. Cryptocurrency is the value that is being exchanged, it is not a security tool.

C) 正确。非对称加密技术允许任何人使用公钥进行消息加密，而加密的消息只能使用正确的私钥进行读取。（文献：A，第2.1章）
Correct. Asymmetric cryptography allows anyone to encrypt a message using a public key, whilst the encrypted message can only be read with the correct private key. (Literature: A, Chapter 2.1)

D) 错误。DLT是区块链的综合技术，它本身并不是安全措施。
Incorrect. DLT is the overall technology of blockchain, it is not a security measure in itself.

区块链以何种方式运用公众见证?

In what way do blockchains use a public witness?

A) 数字法院或图书馆充当公众见证，存储信息以供参考。
A digital courthouse or library acts as a public witness to store information to reference.

B) 区块链网络上的节点证明信息的准确性和真实性。
A node on a blockchain network attests to the accuracy and truthfulness of information.

C) 一个人通过一个公共网络发送一个交易，作为公众见证可以获得奖励。
A person sends a transaction over a public network to earn rewards as a public witness.

D) 可以选择一个首选节点来证明信息的准确性和真实性。
A preferred node can be elected to attest to the accuracy and truthfulness of information.

A) 错误。区块链实质上是一个数字档案馆，但它们不需要一个单独的数字法院或图书馆来充当公正见证。这是节点的作用。
Incorrect. Blockchains are in essence a digital archive, but they do not need a separate digital courthouse or library to act as a public witness. That is what the nodes do.

B) 正确。区块链网络上的每个节点都在见证着信息。所有节点都会在以后的某个日期证明其准确性和真实性，就像法院、图书馆和档案馆是人们储存信息的地方，以便在另一个时间点进行参考一样。(文献:A，第2.4章)
Correct. Each node on a blockchain network witnesses information. All nodes attest to its accuracy and truthfulness at a later date, much like how court houses, libraries and archives are places where people store information to reference at another point in time. (Literature: A, Chapter 2.4)

C) 错误。节点充当公众见证而非个人。节点作为公众见证并不总是获得奖励。
Incorrect. Nodes act as public witnesses, not persons. The nodes do not always earn rewards to act as a public witness.

D) 错误。区块链网络上的每个节点都在见证信息，而不仅仅是首选节点。
Incorrect. Each node on a blockchain network is witnessing information, not just preferred nodes.

区块链实现自我主权身份。

区块链如何做到这一点？

Blockchain enables self-sovereign identity.

How does blockchain do this?

A) 它使中心化的第三方能够提供易于使用和有效的身份信息。
It enables centralized third parties to offer easy-to-use and valid identity information.
B) 它使每个人都可以完全控制自己的金钱、财产和身份。
It enables each person to have exclusive control of their money, property and identity.
C) 它使政府能够轻松地颁发高级数字证书身份。
It enables governments to effortlessly issue identities with advanced digital certificates.
D) 它仅允许互联网公司提供世界一流的安全个人身份存储库。
It enables only internet companies to offer world-class secure personal identity repositories.

A) 错误。集中式系统可能被破坏，文件可能被伪造或更改，这使得身份验证变得困难。2018年，Facebook因向第三方剑桥分析公司分享了8700多万用户的个人数据而登上了新闻头条。这些信息被用来操纵个人的行为。使用的方便性和易用性已经损害了许多人的身份和财务信息。
Incorrect. Centralized systems can be compromised, and documents can be faked or changed, making it difficult to verify identities. Facebook hit the news headlines in 2018 after it shared the personal data of more than 87 million customers with Cambridge Analytica, which is a third party. That information was then used to manipulate individual's behavior. Convenience and ease of use has compromised many people's identities and financial information.
B) 正确。区块链技术允许了自我所有权概念的转变。它点燃了围绕每个人对自己的金钱、财产和身份的专属控制权的道德和自然权利的社会运动的新生命。 （文献：A，第6.1章）
Correct. Blockchain technology has allowed for a shift in the concepts of self-ownership. It has sparked new life into social movements around the moral and natural rights of each person to have exclusive control of their money, property, and identity. (Literature: A, Chapter 6.1)
C) 错误。自我主权的身份是由个人而不是第三方来管理的。一个人可以证明自己，而不是依靠第三方来验证和证实她的证件。
Incorrect. A self-sovereign identity is one that is managed by an individual and not a third party. A person would authenticate herself and not rely on a third party to validate and corroborate her credentials.
D) 错误。只有一小部分公司能够控制网站安全证书的颁发以及管理和培养在线身份。这种中心化使得大量的个人数据存放在集中的服务器上，供每个使用互联网的人使用。这些服务器可以而且确实会受到黑客攻击。
Incorrect. There is only a small group of companies that have control over issuing website security certificates and curating and cultivating online identities. This centralization has caused huge volumes of personal data to be housed on centralized servers for everyone who uses the internet. These servers can and do get hacked.

公有链鼓励用户挖掘区块并保护网络安全。

这是什么激励?

Public blockchains give an incentive to encourage users to mine blocks and secure the network.

What incentive is this?

A) 公有链允许用户创造通证并在二级市场上销售。
Public blockchains allow users to create tokens to sell on secondary markets.
B) 公有链不提供奖励,因为它们是开源的。
Public blockchains do not offer rewards, because they are open source.
C) 公有链为运行挖矿节点提供现金奖励。
Public blockchains offer cash rewards for running mining nodes.
D) 公有链以加密货币的形式提供挖矿奖励。
Public blockchains offer rewards for mining in the form of cryptocurrency.

A) 错误。矿工通常直接赚取加密货币。
Incorrect. Usually, miners earn cryptocurrency directly.
B) 错误。尽管公有链是基于开放式许可证且是开源的,但公有链仍然提供挖矿奖励。
Incorrect. Even though they are based on an open license and are open source, the public blockchains still offer rewards for mining.
C) 错误。矿工收获的是加密货币,而不是常规货币。
Incorrect. Miners are given cryptocurrency, not regular currency.
D) 正确。公有链通常将加密货币作为挖矿的奖励。(文献:A,第1.1章)
Correct. Public blockchains usually give cryptocurrency as a reward for mining. (Literature: A, Chapter 1.1)

一个组织机构想要开发基于区块链技术的智能合约。该组织机构不希望让员工承担维护区块链安全的负担。

什么样的区块链技术**最**适合该组织?

An organization wants to develop smart contracts, based on blockchain technology. The organization does not wish to burden employees with maintaining the security of the blockchain.

What blockchain technology fits the organization **best**?

A) 混合链
A hybrid blockchain

B) 私有链
A private blockchain

C) 公有链
A public blockchain

A) 错误。在混合链中可以控制每个节点的参与级别。如果该组织不希望利用员工保护区块链安全,那么混合链不是最佳选择。
Incorrect. For a hybrid blockchain the level of participation of each node can be controlled. If the organizations do not wish to use its employees to secure the blockchain, this is not the best option.

B) 错误。私有区块链更像是信任网络。网络的成员是已知的,合同可以更改。与基于纸面的业务流程相比,它们提供了改进,但它们没有公共网络那样的不可改变性或可执行性。
Incorrect. Private blockchains are more like trust networks. The members of the network are known, and contracts can be changed. They offer improvements compared to paper-based business processes, but they do not have the same finality or enforceability as public networks.

C) 正确。公有链最大限度地降低更改区块链中智能合约的可能性。公有链的安全不依赖于少数员工,因此符合该组织的期望。(文献:A,第1章和第10.1章)
Correct. A public blockchain minimizes the possibility to change the smart contracts in the blockchain. The security of a public blockchain does not rely on a small number of employees and therefore fits with the organization's wish. (Literature: A, Chapter 1 and 10.1)

超级账本网络的**关键**特点是什么？

What is a **key** characteristic of the Hyperledger network?

A) 它是一个公共区块链网络，也是自2009年以来最古老的网络之一。
It is a public blockchain network and one of the oldest networks, existing since 2009.

B) 它是私有、开源的，可运行个人的分布式账本技术（DLT）。
It is private, open sourced and can run everyone's own distributed ledger technology (DLT).

C) 它利用加密货币作为奖励机制，从而提高网络安全性。
It utilizes cryptocurrency as a reward mechanism, which makes the network more secure.

D) 它利用权益证明（PoS）共识算法作为主要安全措施。
It utilizes the Proof of Stake (PoS) consensus algorithm as its main security measure.

A) 错误。超级账本不是公有链网络，它是由Linux基金会于2015年建立的。
Incorrect. Hyperledger is not a public blockchain network and it was set-up in 2015 by Linux foundation.

B) 正确。超级账本是一个私有但开源的网络，因此可以帮助人们建立自己的DLT。（文献：A，第4.4章）
Correct. Hyperledger is a private but open-sourced network and therefore helps people to spin up their own DLT. (Literature: A, Chapter 4.4)

C) 错误。超级账本并不将加密货币机制用作奖励和用于保证安全性。
Incorrect. Hyperledger does not utilize the cryptocurrency mechanism as rewards and for security.

D) 错误。超级账本不使用PoS共识算法。
Incorrect. Hyperledger does not use the PoS consensus algorithm.

智能合约的**最佳**使用案例是什么?

What is the **best** use case for smart contracts?

A) 使用人工智能（AI）将具有法律约束力的合同数字化和自动化
Digitalize and automate legally binding contracts using artificial intelligence (AI)

B) 使用加密货币在法律体系中强制执行合约
Enforce the execution of contracts in the legal system using cryptocurrencies

C) 通过保险合约中的预定行为或事件确保自动付款
Ensure automatic payments by predetermined actions or events in insurance contracts

D) 将最著名的智能合约平台，即比特币区块链扩展到司法制度
Extend the Bitcoin blockchain, the best-known smart contract platform, to the judicial system

A) 错误。智能合约由开发人员创建，并通过布尔逻辑、数学和加密来强制执行。另一方面，具有法律约束力的合同是由律师创建并由司法系统执行的。大多数智能合约没有法律约束力。AI和智能合约可以一起使用，但这不是最好的用例。
Incorrect. Smart contracts are created by developers and enforced with Boolean logic, mathematics, and encryption. A legally binding contract, on the other hand, is created by a lawyer and enforced by a judicial system. Most smart contracts are not legally binding. AI and smart contracts might be used together, but this is not the best use case.

B) 错误。法律合同由司法系统强制执行；它们与智能合同没有相同的限制。如果违反了向某人付款的法院命令，即使是在民事诉讼中，也有可能被控藐视法庭罪并坐牢，或者资金可以自动从账户中取出。法律更加灵活，软件更加死板。法律和合同是由有法律选择权的人来解释的。代码通常只有一种解释方式，如果它执行时发生意外，则意味着存在需要修复的错误。
Incorrect. Legal contracts are enforced by a judicial system; they do not have the same limitations as smart contracts. If a court order to pay somebody is violated, even in a civil lawsuit, it is possible to be charged with contempt and go to prison, or funds can be automatically withdrawn from an account. Laws are more flexible, and software is more rigid. Laws and contracts are interpreted by people who have legal options. Code is usually only interpreted one way, and if it executes unexpectedly it means there is a bug that needs to be fixed.

C) 正确。农业智能合约可以确保自动支付保险金。如果气温下降损坏了庄稼，农民将得到赔偿。（文献：A，第5.1章）
Correct. A farming smart contract can ensure insurance payments are made automatically. If the temperature goes down and damages crops, the farmer will receive payment. (Literature: A, Chapter 5.1)

D) 错误。比特币区块链的智能合约鲜为人知，但最初提出比特币网络的白皮书暗示了它们的创建。比特币上的智能合约使用的是所谓的"操作码"（opcode），这是彼得·托德（Peter Todd）在比特币改进建议（BIP）65中引入的。
Incorrect. The Bitcoin blockchain is less known for smart contracts, but the white paper that originally proposed the Bitcoin network alluded to their creation. Smart contracts on Bitcoin use what is known as "opcode", which was introduced by Peter Todd as Bitcoin Improvement Proposal (BIP) 65.

在哪种情况下，智能合约是问题的**最佳**解决方案？

In which scenario is a smart contract the **best** solution to the problem?

A) 一个酒保想通过把加密货币转移到他的钱包里来强迫顾客付饮料费。
A bartender wants to force customers to pay for their drinks by transferring cryptocurrency to his wallet.

B) 一位首席财务官希望她的智能手表在她的合作伙伴进入他们的前门时通知她。
A chief financial officer wants her smart watch to notify her when her partner enters their front door.

C) 一个能源公司希望在价格达到预定费率时自动购买电力。
An energy company wants to automatically buy power when the price reaches a predetermined rate.

D) 一个保险公司希望在专案经理认为最佳的情况下向农民付款。
An insurance company wants to pay out a farmer whenever the case manager feels it is best to do so.

A) 错误。在这种情况下，智能合约不会有用。智能合约不会强迫另一方释放资金。
Incorrect. This is not a scenario in which a smart contract would be useful. Smart contracts do not force another party to release funds.

B) 错误。智能合约是两方或多方之间的合约。在这种情况下，没有第二方，因此智能合约不是最好的解决方案。
Incorrect. A smart contract is a contract between two or more parties. In this scenario, there is no second party and therefore a smart contract is not the best solution for this.

C) 正确。这正是智能合约起作用的一个很好的案例。（文献：A，第5.1章）
Correct. This is a good example of a smart contract being useful. (Literature: A, Chapter 5.1)

D) 错误。智能合约由预先确定的事件触发。公司的付款意愿并不是使用智能合约的最佳方式，因为这不会自动触发代码。
Incorrect. Smart contracts get triggered by predetermined events. The willingness of a company to pay is not an optimal way to use a smart contract, because this does not automatically trigger the code.

DApp的用途是什么？

What are DApps designed to do?

A) 在独立应用程序的前端使用业务逻辑执行智能合约
Execute smart contracts with the business logic in the front-end of a standalone application

B) 仅管理加密货币，无需用到治理区块链的任何嵌入式投票系统
Manage cryptocurrencies only, without any embedded voting system for governance of the blockchain

C) 在对等网络（P2P）上运行应用程序，将智能合约的运用范围扩展到简单的价值转移以外
Run applications on a peer-to-peer (P2P) network expanding smart contracts beyond simple value transfer

D) 支持在多个公共云提供商上运行的应用程序，避免任何供应商锁定和欺诈
Support applications that run on multiple public cloud providers avoiding any vendor lock-in and fraud

A) 错误。智能合约是后台，通常只占DApp的一小部分。
Incorrect. Smart contracts are the backend and often only make up a small part of a DApp.

B) 错误。DApp按照功能分为三大类：1）管理财务的DApp；2）利用财务但出于其他目的（例如，游戏）而构建的DApp；3）管理用App，例如投票系统。管理应用程序称为"去中心化自治组织"，通常简称为DAO
Incorrect. DApps are divided into three broad categories based on their function: 1) DApps that manage money; 2) DApps that utilize money but are built for another purpose, such as a game; 3) Apps for governance, such as a voting system. These governance applications are called "decentralized autonomous organizations" which is normally just shortened to DAOs.

C) 正确。DApp将智能合约的运用范围不局限于简单的A到B之间的价值转移。DApp由智能合约构建，但是使用其他服务（例如安全消息），并且通常允许无限数量的参与者在给定规则集中地进行交互。（文献：A，第5.3章）
Correct. DApps expand smart contracts beyond simple A-to-B value transfers. DApps are built with smart contracts but use other services such as secure messaging and often allow an unlimited number of participants to interact within a given rule set. (Literature: A, Chapter 5.3)

D) 错误。DApp是指在P2P网络而非单个系统上运行的应用程序。DApp可以是工具、程序、游戏以及其他可以直接连接用户与提供商的应用。
Incorrect. DApps are applications that run on a P2P network instead of a single system. DApps can be tools, programs, games, and more that connect users and providers directly.

去中心化自治组织(DAO)的作用是什么？

What is the role of a DAO (decentralized autonomous organization)?

A) 通过在商定规则内进行协作和认可的行为来解决委托-代理困境
Address the principal-agent dilemma with collaboration and acceptance of actions within agreed rules

B) 使用公有链将当前的司法系统嵌入受监管的在线智能合约
Embed regulated online smart contracts with the current judicial system, using public blockchains

C) 提供复杂的在线智能合约，无需绑定有形和无形的离线资产
Offer complex online smart contracts without any link to tangible and intangible offline assets

D) 提供一个私有链合约平台，用户可以在该平台上运行其在线应用程序
Provide a private blockchain contract platform on which users can run their online applications

A) 正确。创建DAO概念是为了解决经济学中所谓的"委托代理问题"。委托代理问题是指，当一个"代理人"可代表另一个代理人做出决定，但会受到其自身利益的影响的时候出现的两难困境。"代理人"可选择冒更大的风险，因为他实际上并不承担风险相应的成本。（文献：A，第5.4章）
Correct. The concept of a DAO was created to address what in economics is referred to as the "principal-agent problem". The principal-agent problem is a dilemma that occurs when an "agent" can make decisions on behalf of another agent but is influenced by their own self-interest. The "agent" may choose to take more risk, because they do not actually carry the cost of that risk. (Literature: A, Chapter 5.4)

B) 错误。DAO的代码和功能无法免除个人遵守法律法规的责任。
Incorrect. The code and capabilities of DAOs do not absolve individuals from complying with regulations and laws.

C) 错误。DAO通过其智能合约中编码的规则运行。它们完全在线工作，但可以管理离线资产，例如房地产或自然资源。
Incorrect. DAOs run through rules encoded within their smart contracts. They live completely online but can govern assets that are offline, like real estate or natural resources.

D) 错误。所有公有链都属于DAO。其中包括比特币、以太坊、Factom等。DAO不仅是公共网络，它们可用于管理各种类型的人类组织，例如公司、投资资金，甚至政府。
Incorrect. All public blockchains are DAOs. These include Bitcoin, Ethereum, Factom, and others. DAOs can be more than public networks. They can be used to manage all types of human organizations such as corporations, investment funds, or even governments.

区块链技术如何能够**最好地**帮助保护身份数据安全？

How can blockchain technology **best** help securing identity data?

A) 通过在用户服务器上提供安全数据存储来免除第三方介入
By eliminating third parties through providing secured-data storage at a user's server
B) 将所有健康数据编码并保存在私有、非许可链中
By encoding all the health data and save it on a private and permissionless blockchain
C) 通过使用加密算法保护已在互联网上提交的数据
By protecting data that has been submitted on the internet using a cryptographic algorithm
D) 提供个人数据信息而不披露能够证明其真实性的实际数据
By providing information personal data without disclosing the actual data that proves it

A) 错误。在用户服务器使用区块链根本没有意义。区块链应该是一个分布式账本。
Incorrect. It makes no sense to use a blockchain at the user's server. Blockchain is supposed to be a distributed ledger.
B) 错误。在非许可链上对个人数据进行编码毫无意义，因为非许可链的安全性不足。
Incorrect. Encoding personal data at a permissionless blockchain makes no sense as a permissionless blockchain is not well-enough secured for this.
C) 错误。保护已在互联网上提交的信息毫无意义，因为该信息可能已遭破坏。
Incorrect. It makes no sense to protect information that has been submitted on the internet before, as it might have been compromised already.
D) 正确。提供信息而不披露实际数据是区块链的重要功能之一。（文献：A，第6.1章）
Correct. Providing information without disclosing the actual data is one of the important functions of a blockchain. (Literature: A, Chapter 6.1)

将区块链网络与物联网（IoT）结合的价值是什么？

What is the value of using blockchain networks with Internet of Things (IoT)?

A) 允许区块链用户跟随和访问自动驾驶汽车
Allowing blockchain users to follow self-driving cars and access these cars

B) 使用存储在区块链上的安全身份避免电子欺骗攻击
Avoiding a spoofing attack using the secured identity that is stored on a blockchain

C) 启用可自行编程的软件，可无需人工干预解决问题
Enabling software that programs itself to solve problems without human intervention

D) 使用超级账本Fabric挖矿解决昂贵而复杂的计算
Solving expensive and complex calculations using Hyperledger Fabric mining

A) 错误。这将会造成危险境地，自动驾驶汽车容易受到电子欺骗攻击或黑客攻击。有许多公司正在开发利用区块链保护IoT设备的技术。
Incorrect. This would be a dangerous situation where self-driving cars would be open to spoofing attacks or hacks. There are many companies developing technologies that utilize blockchain to protect IoT devices.

B) 正确。IoT可以利用区块链安全身份防止电子欺骗攻击，以免恶意方冒充另一台设备发起攻击，从而窃取数据或引起某种混乱。（文献：A，第6.3章）
Correct. IoT can utilize blockchain secured identity to prevent a spoofing attack where a malicious party impersonates another device to launch an attack to steal data or cause some other disorder. (Literature: A, Chapter 6.3)

C) 错误。这是区块链网络与人工智能（AI）结合的价值。
Incorrect. This is the value of using blockchain networks with artificial intelligence (AI).

D) 错误。超级账本Fabric中不存在挖矿。矩阵AI提供了一种解决方案，可以轻松地将机器学习与智能合约相结合。该平台修改了智能合约的执行方式，并提高了智能合约的速度、灵活性、便捷性和安全性。矩阵利用其挖矿算力解决昂贵、复杂的AI计算。
Incorrect. There is no mining in Hyperledger Fabric. Matrix AI is providing a solution that makes it easy to combine machine learning and smart contracts. The platform modifies how smart contracts are executed, and improves their speed, flexibility, ease and security. Matrix uses its mining power to solve expensive and complex AI computations.

区块链技术实现了去中心化市场。

去中心化市场有什么好处？

Blockchain technology has made decentralized marketplaces possible.

What is a benefit of a decentralized marketplace?

A) 它基于开源技术，因此使用时无需任何投资。
It is based on open-source technology, so it can be used without any investment.

B) 它无需付费的许可证就可以经营，因此可以得到更好的管理。
It is not under a paid license to operate and therefore it is managed better.

C) 因使用加密货币，它的成本相对较低，而且非常容易访问。
It is relatively cheap due to the use of cryptocurrency and is very accessible.

D) 由于智能合约，它具有防篡改功能，抗关闭能力，以及可信赖性。
It is tamper-proof, resilient to being shut down and trustworthy due to smart contracts.

A) 错误。使用开源技术不能确定是否需要投资。此外，并非所有的区块链都基于开源代码。
Incorrect. The use of open-source technology does not determine whether investment is needed. Moreover, not all blockchains are based on open-source code.

B) 错误。获得付费许可证不能决定产品的管理好坏。
Incorrect. Being under a paid license does not determine whether a product is managed well.

C) 错误。去中心化市场的成本不一定低于其他市场。
Incorrect. It is not necessarily true that decentralized marketplaces are cheaper than other marketplaces.

D) 正确。区块链可确保每个人都是自己所表述的身份，无需第三方即可保证价值转移的安全。（文献：A，第6.5章）
Correct. The blockchain ensures that everyone is who they say they are and secures the transfer of value, without the need for a third party. (Literature: A, Chapter 6.5)

区块链如何改善供应链？

How does blockchain improve supply chains?

A) 通过自动创建双方之间的贸易协议
By automatically creating trade agreements between two parties
B) 通过创建安全的集中化市场进行商品交易
By creating safe centralized marketplaces to trade goods on
C) 通过稳定相关国家的本国货币
By stabilizing the national currencies of the countries involved
D) 通过软件系统转移通证化所有权
By transferring tokenized ownership through a software system

A) 错误。贸易协议可编程为智能合约，但是区块链无法创建贸易协议。
Incorrect. Trade agreements can be programmed into smart contracts, but blockchain does not create these.
B) 错误。区块链可以帮助加强去中心化市场的安全性，但根本无法帮助创建集中化市场。
Incorrect. Blockchain can help making decentralized marketplaces more secure, but it definitely does not help to create centralized marketplaces.
C) 错误。区块链无助于稳定本国货币。
Incorrect. Blockchain does not help stabilizing national currencies.
D) 正确。区块链可以仅通过软件系统转移价值或通证化所有权（文献：A，第7.1章）
Correct. Blockchain can transfer value, or tokenized ownership through just a software system. (Literature: A, Chapter 7.1)

新加坡金融管理局（MAS）与区块链公司R3合作。

双方共同取得了什么成就？

The Monetary Authority of Singapore (MAS) and blockchain company R3 partnered together.

What did they achieve together?

A) 创建了智能合约和稳定币
The creation of smart contracts and stable coins
B) 促进了银行间消息传递
The facilitation of interbank transmission of messages
C) 不受时区限制的首次跨行支付
The first interbank payments without limitations of time zones
D) 发布采用加密技术的电汇
The launch of wire transfers using cryptography

A) 错误。Everex参与了智能合约和稳定币的开发，以支持商业和中央银行的数字货币计划。
Incorrect. Everex is involved in the development of smart contracts and stable coins to support the digital currency initiatives of commercial and central banks.
B) 错误。环球银行金融电信协会（SWIFT）的全球网络已成为负责大多数国际支付的实体。尽管该网络不转移资金，但其促进了银行间的消息传输，有效地允许银行进行直接通信，从而简化了国际汇款流程。
Incorrect. The global network for the Society of Worldwide Interbank Financial Telecommunication (SWIFT) became the entity responsible for most international payments. Although it does not move money, the network facilitates the transmission of messages between banks, effectively allowing banks to get in direct communication to make the international money transfer process easier.
C) 正确。MAS与区块链公司R3合作，2016年利用区块链技术进行了首次跨行支付。该项目表明，银行可以全天候交易和结算，不再受时区和营业时间的限制。（文献：A，第7.2章）
Correct. The MAS partnered with blockchain company R3 and conducted the first interbank payments using blockchain technology in 2016. The project showed that banks could transact and settle round-the-clock and were no longer limited by time zones and office hours. (Literature: A, Chapter 7.2)
D) 错误。西联汇款（Western Union）成立后发布了电汇。此过程通过电报网络，实现个人或实体间的电子资金转账，有效地帮助在境内和跨境转移资金。西联汇款仍处理全球大部分个人汇款。
Incorrect. Western Union was founded, and they launched the wire transfer. This process uses electronic funds transfer from one person or entity to another through its telegraph network, effectively helping to move money within and across borders. Western Union still handles the majority of personal remittances globally.

什么是法定数字货币？

What is digital fiat currency?

A) 代表一个国家财政储备的货币的数字形式
A digital form of currency, that represents a country's financial reserves
B) 一种创建透明且无国界债务市场的电子货币
An e-currency, that creates a transparent and borderless debt market
C) 一种无需银行账户即可进行交易的在线系统
An online system, that enables making transactions without a bank account

A) 正确。法定数字货币是指特定国家货币的数字形式，由本国货币主管机构发行和监管。（文献：A，第8.1章）
Correct. Digital fiat currency is defined as the representation in the digital form of a currency of a particular nation and is issued and regulated by the competent monetary authority of the country. (Literature: A, Chapter 8.1)
B) 错误。法定数字货币与债务市场无关。
Incorrect. Digital fiat currency has nothing to do with debt markets.
C) 错误。法定数字货币仅适用于持有银行账户的人。它针对的是国际收支余额，而非个人交易。
Incorrect. Digital fiat currency works only for people with a bank account. It is aimed at international payment balance, not individual transactions.

区块链技术如何使保险业受益？

How does blockchain technology benefit the insurance industry?

A) 避免了国家主管部门的合规性要求，从而减少了开销
By avoiding compliance requirements of national authorities, which reduces overhead
B) 确保了数据的准确性和实现小额保险自动化，从而降低了成本
By ensuring accuracy of data and automating micro insurances, which reduces costs
C) 引入了客户支付灵活的保费，从而增加利润
By introducing flexible premiums to be paid by customers, which increases profits
D) 设置了数字付款方式，从而简化了理赔
By setting up a digital mode of payment, which simplifies claims settlement

A) 错误。区块链活动必须遵守法律法规。
Incorrect. Blockchain activities must comply with legislation and regulations.
B) 正确。区块链技术使保险公司能够为现有的客户提供更多价值。（文献：A，第8.3章）
Correct. Blockchain technology enables insurance companies to provide more value to the contacts they already have. (Literature: A, Chapter 8.3)
C) 错误。区块链并未定义客户保费。
Incorrect. Blockchain does not define the premium for customers.
D) 错误。区块链并未定义向保险公司付款的方式。
Incorrect. Blockchain does not define the mode of payment to the insurance company.

区块链技术如何帮助保护知识产权(IP)?

How does blockchain technology help to protect intellectual property rights (IP)?

A) 它允许用户将IP交易包括在智能合约中。
It allows a user to include IP transactions in smart contracts.

B) 它允许用户记录事件并建立时间线。
It allows a user to record an event and establish the timeline.

C) 它允许用户记录软件包的创建。
It allows a user to record the creation of software packages.

D) 它允许用户发送交易和获得IP所有权。
It allows a user to send a transaction and receive IP ownership.

A) 错误。智能合约充当两方或多方之间的在线合约。智能合约是数字协议或者控制IP访问的规则集。
Incorrect. A smart contract acts as an online contract between two or more parties. Smart contracts are digital agreements or sets of rules governing the IP access.

B) 正确。IP的基础是公平的概念，"谁在什么时候做了什么"，第一个做了某事的人应有权享有相关工作的商业利益。利用区块链可以确定某个事物在给定时间点内存在，第三方可以对该信息进行验证。（文献：A，第8.4章）
Correct. IP is grounded in a concept of fairness, "who did what when" and the first person that did something should have the right to the commercial benefit for those efforts. Using blockchain, it is possible to establish that something existed at a given point in time and third parties can verify that information. (Literature: A, Chapter 8.4)

C) 错误。区块链技术用于记录有关IP创建的事件。
Incorrect. Blockchain technology is used to record an event regarding creation of an IP.

D) 错误。仅发送交易不可能确立IP所有权。
Incorrect. It is not possible to establish ownership over an IP by simply sending a transaction.

哪一项属于政府积极促进区块链应用的案例?

What is an example of how a government is actively promoting the use of blockchain?

A) 中国创建了一个监管沙盒，允许他们密切监控区块链挖矿中的实验，并创建各自的加密货币。
China has created a regulatory sandbox that allows them to closely monitor the experiments in blockchain mining and create their own cryptocurrency.

B) 爱沙尼亚提供电子居留权（e-Residency）软件，世界上任何有兴趣在网上和欧盟内部经营企业的人都可以使用。
Estonia offers e-Residency software, which is available to anyone in the world interested in operating a business online and from within the European Union.

C) 新加坡金融管理局(MAS)正在使用分布式账本技术(DLT)为银行间支付创造中央银行数字货币。
Singapore's Monetary Authority (MAS) is creating central bank digital money for payments between banks using distributed ledger technology (DLT).

A) 错误。中国没有自己的加密货币。
Incorrect. China does not have its own cryptocurrency.

B) 错误。爱沙尼亚为在线服务推出了数字身份证，并作为第一个提供电子居留权的国家提供了公民身份服务。他们创造了一个数字身份，世界上任何有兴趣在网上和通过欧盟经营企业的人都可以使用。然而，电子居留权并不是分布式的软件。它也不仅仅是在推广区块链技术。
Incorrect. Estonia launched digital ID cards for online services and has offered citizenship as a service by being the first country to offer e-Residency. They create a digital identity, available to anyone in the world interested in operating a business online and through the European Union. However, the e-Residency is not software that is distributed. It is also not solely promoting blockchain technology.

C) 正确。MAS正在使用分布式账本技术创建中央银行数字货币。该项目的第一阶段始于2016年，他们证明了使用中央银行发行的等同于新加坡元（SGD）的通证进行国内银行间支付的能力。（文献：A，第9.2章）
Correct. The MAS are creating central bank digital money using DLT. The first phase of the project started in 2016 where they proved the ability to conduct a domestic inter-bank payment using a central bank-issued Singapore Dollar (SGD) equivalent token. (Literature: A, Chapter 9.2)

为什么将区块链描述为可增加互联网信任度的技术?

Why is blockchain described as the technology that adds a layer of trust to the internet?

A) 区块链允许个人和团体一起工作，而不必相互信任或建立权威。
It allows individuals and groups to work together without having to trust each other or establish authority.

B) 区块链创建两方或多方之间的虚拟专用网络（VPN）隧道，以进行在线转账。
It creates a dedicated virtual private network (VPN) tunnel between two or more parties to carry out online fund transfers.

C) 区块链提供了一种机制，使政府可以创建自己的法定数字货币来代替实物货币。
It provides mechanism for the government to create their own digital fiat currency as a replacement of physical currency.

D) 区块链提供了多因素身份验证，可以安全地创建和更新加密货币交易记录。
It provides multifactor authentication to create and update records of cryptocurrency transactions securely.

A) 正确。区块链允许个人、政府和企业以公平和开放的方式合作，不需要先建立信任、所有权和权威。（文献：A，第9.4章）
Correct. It allows for individuals, governments, and businesses to work together in a fair and open manner, without first establishing trust, ownership, and authority. (Literature: A, Chapter 9.4)

B) 错误。VPN不是区块链技术的应用。
Incorrect. VPN is not an application of blockchain technology.

C) 错误。法定数字货币是区块链技术的应用之一。
Incorrect. Digital fiat currency is one of the applications of blockchain technology.

D) 错误。区块链技术利用加密哈希函数提供了不可篡改的特性。
Incorrect. Blockchain technology makes use of cryptographic hash functions to provide the trait of immutability.

试题评分

如下表格为本套样题的正确答案，供参考使用。

问题	答案	问题	答案
1	C	21	C
2	C	22	B
3	C	23	B
4	C	24	D
5	D	25	C
6	B	26	B
7	D	27	C
8	A	28	C
9	D	29	C
10	A	30	A
11	C	31	D
12	H	32	B
13	C	33	D
14	D	34	D
15	D	35	C
16	C	36	A
17	A	37	B
18	C	38	B
19	C	39	C
20	A	40	A

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH