IS6200 期末考试问题整理与答案

1. 货币相关问题

问题 1: What is money?

Money is a medium of exchange, unit of account, and store of value used to facilitate transactions and economic activities.
货币是用于促进交易和经济活动的交换媒介、记账单位和价值储存手段。

问题 2: What are the three important functions of money?

The three important functions of money are:

1. Medium of Exchange: Used to buy goods and services.
2. Unit of Account: Provides a standard measure of value.
3. Store of Value: Retains value over time for future use.
   货币的三个重要功能是：
4. 交换媒介：用于购买商品和服务。
5. 记账单位：提供价值的标准衡量。
6. 价值储存：随时间保留价值以供未来使用。

问题 3: Do you think cryptocurrencies are good money?

Cryptocurrencies like Bitcoin are partially good money, serving as a medium of exchange and store of value, but their volatility and limited acceptance hinder their role as a stable unit of account. Stablecoins like USDT better fulfill money's functions due to price stability.
像比特币这样的加密货币在某种程度上是好的货币，可作为交换媒介和价值储存，但波动性和有限接受度限制了其作为稳定记账单位的作用。像 USDT 这样的稳定币因价格稳定更能履行货币功能。

2. 比特币相关问题

问题 4: How do we secure our own accounts?

Bitcoin accounts are secured using public-private key cryptography, where the private key, kept secret, signs transactions to prove ownership, and losing it results in loss of funds.
比特币账户通过公钥-私钥加密技术保护，用户保密的私钥用于签名交易以证明所有权，丢失私钥会导致资金无法访问。

问题 5: Who should keep the ledger?

In Bitcoin, the ledger is maintained by a decentralized network of nodes, primarily miners, who validate and record transactions in the blockchain without a single controlling entity.
在比特币中，账本由去中心化的节点网络维护，主要由矿工验证并记录交易到区块链中，没有单一实体控制。

问题 6: How should we trust the ledger maintainer?

Trust in Bitcoin's ledger is achieved through Proof of Work (PoW) consensus, where miners compete to solve costly computational puzzles, making manipulation economically impractical.
比特币账本的信任通过工作量证明（PoW）共识机制实现，矿工竞争解决高成本计算难题，操纵账本经济上不可行。

问题 7: How do we protect ourselves from attacks?

Bitcoin protects against attacks via Proof of Work, requiring attackers to control over 50% of mining power (51% attack), which is costly and impractical due to high energy demands.
比特币通过工作量证明防御攻击，攻击者需控制超过50%的算力（51%攻击），因高能耗成本高昂且不现实。

问题 8: How does this help privacy?

Bitcoin's public-private key system provides pseudonymity, linking transactions to addresses rather than real identities, offering some privacy unless linked to personal information.
比特币的公钥-私钥系统提供伪匿名性，交易与地址而非真实身份相关联，除非与个人信息关联，否则提供一定隐私。

问题 9: Does this conflict with transparency?

Bitcoin's pseudonymity does not conflict with transparency, as the blockchain is fully public, allowing anyone to verify transactions while protecting user identities.
比特币的伪匿名性与透明性不冲突，区块链完全公开，任何人都可验证交易，同时保护用户身份。

问题 10: Why or why not?

Bitcoin balances privacy and transparency: pseudonymous addresses protect user identities (privacy), while the public blockchain ensures verifiable transactions (transparency).
比特币平衡了隐私和透明性：伪匿名地址保护用户身份（隐私），公开区块链确保交易可验证（透明性）。

问题 11: How does Zcash change this landscape?

Zcash enhances privacy over Bitcoin by using zero-knowledge proofs (zk-SNARKs) to hide transaction details (sender, receiver, amount) while allowing public verification of validity.
Zcash 通过零知识证明（zk-SNARKs）增强了对比特币的隐私，隐藏交易细节（发送者、接收者、金额），同时允许公开验证交易有效性。

问题 12: What is the main difference between Zcash and Bitcoin?

The main difference is privacy: Bitcoin offers pseudonymity with transparent transactions, while Zcash uses zk-SNARKs for optional shielded transactions, hiding details.
主要区别是隐私：比特币提供伪匿名性，交易透明；Zcash 使用 zk-SNARKs 提供可选屏蔽交易，隐藏细节。

问题 13: Proof of Work? How do you describe this in your own words?

Proof of Work (PoW) is a consensus mechanism where miners solve complex mathematical puzzles to validate transactions and secure the blockchain through computational effort.
工作量证明（PoW）是一种共识机制，矿工通过解决复杂数学难题验证交易并通过计算消耗保护区块链安全。

问题 14: Why are miners willing to spend so much electricity in doing that?

Miners spend electricity on Proof of Work to earn block rewards (newly minted Bitcoins) and transaction fees, which incentivize their costly computational efforts.
矿工在工作量证明上耗费电力是为了获得区块奖励（新铸造的比特币）和交易费用，这些激励他们进行高成本计算。

问题 15: What is the difficulty of the genesis block?

The difficulty of Bitcoin's genesis block, created on January 3, 2009, was set to the minimum value of 1, as it was the first block.
比特币创世区块（2009 年 1 月 3 日创建）的难度设为最低值 1，因为它是首个区块。

问题 16: Can you recall two types of scaling solutions?

Two types of scaling solutions for Bitcoin are:

1. Layer 1 (On-Chain): Modifying the protocol, e.g., SegWit to increase block capacity.
2. Layer 2 (Off-Chain): Processing transactions off-chain, e.g., Lightning Network.
   比特币的两种扩展解决方案是：
3. 第一层（链上）：修改协议，例如 SegWit 增加区块容量。
4. 第二层（链下）：链下处理交易，例如闪电网络。

问题 17: What's SegWit? What's the original problem that it tried to solve?

SegWit (Segregated Witness) is a Bitcoin upgrade that separates signature data from transaction data, increasing block capacity and fixing transaction malleability to enable Layer 2 solutions like the Lightning Network.
SegWit（隔离见证）是比特币升级，将签名数据与交易数据分离，增加区块容量并修复交易可塑性，支持如闪电网络的第二层解决方案。

问题 18: What's Lightning Network?

The Lightning Network is a Layer 2 scaling solution for Bitcoin, enabling fast, low-cost off-chain transactions via payment channels, settling final balances on-chain.
闪电网络是比特币的第二层扩展解决方案，通过支付通道实现快速、低成本链下交易，最终余额在链上结算。

问题 19: What's Taproot?

Taproot is a 2021 Bitcoin soft fork introducing Schnorr signatures and MAST to enhance privacy and efficiency, making complex transactions appear like regular ones.
Taproot 是 2021 年的比特币软分叉，引入 Schnorr 签名和 MAST，提升隐私和效率，使复杂交易看起来像普通交易。

问题 20: What is "ordinals"? How does it change the Bitcoin ecosystem?

Ordinals inscribe data on individual satoshis, enabling NFTs and expanding Bitcoin's use cases beyond payments to include digital collectibles and art.
Ordinals 将数据铭刻在单个聪上，支持 NFT，扩展了比特币的用例，超越支付，涵盖数字收藏品和艺术。

3. 加密技术相关问题

问题 21: What is encryption?

Encryption is the process of converting plaintext into ciphertext using a key to protect data confidentiality, accessible only to authorized parties.
加密是使用密钥将明文转换为密文的过程，以保护数据机密性，仅授权方可访问。

问题 22: Symmetric vs. Asymmetric?

Symmetric encryption uses one key for encryption and decryption (e.g., AES), fast but requires secure key sharing. Asymmetric encryption uses a public-private key pair (e.g., RSA), slower but secure for key exchange.
对称加密使用单一密钥进行加密和解密（例如 AES），速度快但需安全共享密钥。非对称加密使用公钥-私钥对（例如 RSA），速度慢但适合密钥交换。

问题 23: What is a hash function?

A hash function is a one-way function mapping data to a fixed-size output (hash) to ensure data integrity, being deterministic, collision-resistant, and irreversible.
哈希函数是一种单向函数，将数据映射到固定大小的输出（哈希），确保数据完整性，具有确定性、抗碰撞性和不可逆性。

问题 24: Know some basic properties of cryptographic hash functions

Basic properties of cryptographic hash functions include:

1. Deterministic: Same input produces the same hash.
2. Collision Resistance: Hard to find two inputs with the same hash.
3. Preimage Resistance: Hard to reverse the hash to the original input.
   加密哈希函数的基本属性包括：
4. 确定性：相同输入产生相同哈希。
5. 抗碰撞性：难以找到两个输入产生相同哈希。
6. 原像抗性：难以逆向哈希找到原始输入。

问题 25: What’s its difference from encryption?

Hash functions are one-way, producing a fixed-size output to verify integrity, and are irreversible, while encryption is reversible to protect confidentiality using keys.
哈希函数是单向的，生成固定大小输出以验证完整性，不可逆；加密是可逆的，使用密钥保护机密性。

问题 26: How about digital signature?

A digital signature uses asymmetric cryptography (private key to sign, public key to verify) to ensure authenticity, integrity, and non-repudiation of messages or transactions.
数字签名使用非对称加密（私钥签名，公钥验证），确保消息或交易的真实性、完整性和不可否认性。

问题 27: How it works?

A digital signature works by hashing a message, signing the digest with the sender’s private key, and verifying it with the public key to ensure the message is unchanged and authentic.
数字签名通过哈希消息，用发送者私钥签名摘要，并用公钥验证，确保消息未更改且真实。

问题 28: Why we need it? (or how is it better than our traditional wet ink signature?)

Digital signatures provide cryptographic proof of authenticity, integrity, and non-repudiation, making them harder to forge and more secure than wet ink signatures for digital transactions.
数字签名提供真实性、完整性和不可否认性的加密证明，比湿墨签名更难伪造，在数字交易中更安全。

4. 以太坊相关问题

问题 29: What's added in Ethereum such that it can achieve things that Bitcoin is incapable of?

Ethereum adds smart contracts, programmable code in a Turing-complete language, enabling complex applications like DeFi and DAOs beyond Bitcoin's payment focus.
以太坊添加了智能合约，即图灵完备语言的可编程代码，支持复杂应用（如 DeFi 和 DAO），超越比特币的支付功能。

问题 30: What new feature we need to go beyond payment only?

Smart contracts are needed, allowing programmable, self-executing agreements for applications like lending, voting, and token creation.
需要智能合约，支持可编程、自动执行的协议，用于借贷、投票和代币创建等应用。

问题 31: How do we safeguard the network while adding this new feature?

Ethereum safeguards smart contracts with the Gas mechanism, limiting computational resources, preventing infinite loops, and charging fees to deter malicious code.
以太坊通过 Gas 机制保护智能合约，限制计算资源，防止无限循环，并收取费用阻止恶意代码。

问题 32: Can we predict whether a program will stop within a finite amount of time?

No, the halting problem proves it's impossible to predict whether a program will stop in finite time for all cases, so Ethereum uses Gas limits.
不能，停机问题证明无法预测程序是否在有限时间内停止，因此以太坊使用 Gas 限制。

问题 33: Can you program/code in Bitcoin?

Bitcoin supports limited programming via its scripting language (e.g., for multi-signature transactions), but it's not Turing-complete, unlike Ethereum's smart contracts.
比特币通过脚本语言支持有限编程（例如多重签名交易），但非图灵完备，与以太坊的智能合约不同。

问题 34: What's not good?

Bitcoin's scripting language is limited, not Turing-complete, and lacks flexibility for complex applications like DeFi or DAOs, restricting it to payments.
比特币的脚本语言受限，非图灵完备，缺乏复杂应用（如 DeFi 或 DAO）的灵活性，仅限支付功能。

问题 35: What is the halting problem?

The halting problem proves no algorithm can determine whether any program will halt or run indefinitely for all inputs.
停机问题证明没有算法能确定任意程序对所有输入是否会停止或无限运行。

问题 36: And how does Ethereum deal with it?

Ethereum deals with the halting problem by enforcing Gas limits on smart contract execution, stopping programs that exceed allocated resources.
以太坊通过对智能合约执行设置 Gas 限制处理停机问题，停止超出分配资源的程序。

问题 37: What's finality?

Finality is the assurance that a blockchain transaction is permanently confirmed and cannot be reversed, achieved through consensus mechanisms.
确定性是区块链交易被永久确认且不可逆的保证，通过共识机制实现。

问题 38: How's finality different between PoW and PoS?

In PoW (e.g., Bitcoin), finality is probabilistic, requiring multiple confirmations to reduce reversal risk. In PoS (e.g., Ethereum post-Merge), finality is deterministic after validator attestations.
在 PoW（如比特币）中，确定性是概率性的，需多个确认降低逆转风险。在 PoS（如合并后以太坊）中，确定性在验证者证明后确定。

问题 39: Recall that one may launch 34% attack in PoS. What are the attacks and how can we counteract such attacks?

A 34% attack in PoS involves controlling one-third of validators to disrupt consensus (e.g., delay finality); countermeasures include slashing malicious validators' stakes and social coordination.
PoS 中的 34% 攻击涉及控制三分之一验证者干扰共识（例如延迟确定性）；对策包括削减恶意验证者的质押和社交协调。

问题 40: What is Gas in Ethereum? Why is it needed?

Gas is Ethereum's transaction fee unit, needed to limit computational resources, prevent infinite loops (halting problem), and deter malicious code execution.
Gas 是以太坊的交易费用单位，用于限制计算资源，防止无限循环（停机问题），并阻止恶意代码执行。

问题 41: What is "optimistic rollup"?

Optimistic Rollup is a Layer 2 scaling solution for Ethereum that processes transactions off-chain, assuming validity, and posts compressed data on-chain with fraud proofs.
乐观 Rollup 是以太坊的第二层扩展解决方案，链下处理交易，假设有效，将压缩数据发布到链上并使用欺诈证明。

问题 42: What does it mean by "optimistic" here?

"Optimistic" means transactions are assumed valid, processed off-chain, and only challenged via fraud proofs if disputes arise, reducing on-chain computation.
"乐观"指交易默认被假设有效，在链下处理，仅在争议时通过欺诈证明挑战，减少链上计算。

问题 43: How can we guarantee the validity of transactions submitted via rollup?

Validity is guaranteed by fraud proofs, allowing anyone to challenge invalid transactions within a dispute period, reverting them if proven invalid.
通过欺诈证明保证交易有效性，任何人在争议期内可挑战无效交易，若证明无效则撤销。

问题 44: What're the differences between rollup and the Lightning Network?

Rollup processes general Ethereum transactions (e.g., smart contracts) off-chain with fraud or ZK proofs, while Lightning Network focuses on Bitcoin payment channels, settling balances on-chain.
Rollup 链下处理以太坊通用交易（例如智能合约），使用欺诈或零知识证明；闪电网络专注于比特币支付通道，链上结算余额。

问题 45: What happened in the 2016 DAO hack? What was the bug? What did the developers do to fix the bug?

The 2016 DAO hack exploited a reentrancy bug, allowing an attacker to drain 3.6 million ETH; developers hard-forked Ethereum to recover funds, creating Ethereum Classic.
2016 年 DAO 黑客攻击利用重入漏洞，攻击者窃取 360 万 ETH；开发者硬分叉以太坊恢复资金，创建了以太坊经典。

问题 46: How did it happen?

The DAO hack exploited a reentrancy vulnerability, where a malicious contract repeatedly called the withdrawal function before the balance updated, draining funds.
DAO 黑客攻击利用重入漏洞，恶意合约在余额更新前反复调用提款函数，耗尽资金。

问题 47: What is the vulnerability that results in the hack?

The vulnerability was reentrancy, allowing a malicious contract to repeatedly call back into the DAO's withdrawal function before updating the balance.
漏洞是重入，恶意合约在更新余额前反复回调 DAO 的提款函数。

问题 48: How could we solve it?

Reentrancy can be solved by using mutex locks, updating state before external calls, or using checked functions like `transfer` instead of `call`.
重入问题可通过使用互斥锁、在外部调用前更新状态或使用 `transfer` 而非 `call` 的检查函数解决。

问题 49: What's the consequence to Ethereum?

The DAO hack led to a hard fork, splitting Ethereum into Ethereum (ETH, reversing the hack) and Ethereum Classic (ETC, preserving the original chain).
DAO 黑客攻击导致硬分叉，将以太坊分裂为以太坊（ETH，撤销黑客攻击）和以太坊经典（ETC，保留原始链）。

问题 50: Ethereum shifted from PoW to PoS. What is PoS (in Ethereum)? Is it better than PoW?

PoS in Ethereum uses staked ETH for validator consensus, reducing energy use compared to PoW, which is more efficient but faces "nothing at stake" risks.
以太坊的 PoS 使用质押 ETH 进行验证者共识，比 PoW 更节能，但面临"无利害关系"风险。

问题 51: What does it mean by "nothing at stake" in a PoS blockchain network like Ethereum?

"Nothing at stake" means PoS validators risk no loss for supporting invalid chains, potentially disrupting consensus, mitigated by slashing penalties.
"无利害关系"指 PoS 验证者支持无效链无损失，可能干扰共识，通过削减惩罚缓解。

问题 52: Is the shift from PoW to PoS a layer 1 or layer 2 scaling solution?

The PoW to PoS shift is a Layer 1 scaling solution, altering Ethereum's core consensus protocol.
PoW 到 PoS 的转变是第一层扩展解决方案，改变了以太坊的核心共识协议。

5. DAO 相关问题

问题 53: What is the full name of "DAO"?

DAO stands for Decentralized Autonomous Organization, a blockchain-based entity governed by smart contracts and community voting without central authority.
DAO 的全称是去中心化自治组织，基于区块链、通过智能合约和社区投票治理，无中央权威。

问题 54: What is the principal-agent problem? What are the agency costs?

The principal-agent problem occurs when agents prioritize self-interest over principals; agency costs are expenses to monitor and align interests.
代理问题指代理人优先考虑自身利益而非委托人；代理成本是监控和对齐利益的费用。

问题 55: What is the agency conflict? How does DAO mitigate this problem?

Agency conflict arises when agents favor their interests over principals. DAOs mitigate this through transparent smart contracts and community voting to align incentives.
代理冲突指代理人优先自身利益而非委托人。DAO 通过透明智能合约和社区投票对齐激励，减轻此问题。

问题 56: How do DAOs mitigate this agency conflict?

DAOs mitigate agency conflict by using transparent, automated smart contract governance and community voting to reduce centralized control and align interests.
DAO 通过透明、自动化的智能合约治理和社区投票减少集中控制，对齐利益，减轻代理冲突。

问题 57: What are the new challenges?

New DAO challenges include low voter participation, smart contract vulnerabilities (e.g., DAO hack), and uncertain regulatory compliance.
DAO 的新挑战包括投票参与度低、智能合约漏洞（例如 DAO 黑客攻击）和不确定的监管合规性。

问题 58: What are some common voting approaches?

Common DAO voting approaches include token-based (weighted by token holdings), quadratic (votes cost quadratically), and reputation-based voting.
DAO 常见的投票方式包括基于代币（按代币持有量加权）、二次方（投票成本二次方增长）和基于声誉的投票。

问题 59: What’s quadratic voting?

Quadratic voting is a system where vote costs increase quadratically (e.g., 1 vote costs 1 token, 2 votes cost 4 tokens), balancing influence and reducing wealthy voter dominance.
二次方投票是一种投票系统，投票成本呈二次方增长（例如 1 票成本 1 代币，2 票成本 4 代币），平衡影响力和减少富裕投票者主导。

问题 60: Does it prevent Sybil attack?

Quadratic voting partially mitigates Sybil attacks by increasing the cost of multiple identities, but additional measures like identity verification are needed.
二次方投票通过增加多个身份的成本部分缓解 Sybil 攻击，但需额外身份验证措施。

6. Hyperledger Fabric 相关问题

问题 61: Why are Bitcoin/Ethereum-like blockchains not ideal for most business applications?

Bitcoin and Ethereum are public, permissionless blockchains with slow speeds, high costs, and public data, unsuitable for businesses needing privacy and compliance. Hyperledger Fabric, a permissioned blockchain, addresses these.
比特币和以太坊是公共、无许可区块链，速度慢、成本高、数据公开，不适合需要隐私和合规的企业。Hyperledger Fabric 作为许可制区块链解决这些问题。

问题 62: How does frameworks like Fabric facilitate the adoption of blockchain into businesses?

Hyperledger Fabric provides modular, permissioned blockchain frameworks with privacy, scalability, and customizable consensus, enabling secure business adoption.
Hyperledger Fabric 提供模块化、许可制区块链框架，具有隐私性、可扩展性和可定制共识，促进企业安全采用区块链。

问题 63: What is a channel in a Fabric network?

A channel is a private subnet in Hyperledger Fabric with a separate ledger, allowing only channel members to access confidential transactions and data.
通道是 Hyperledger Fabric 中的私有子网络，拥有独立账本，仅允许通道成员访问机密交易和数据。

问题 64: What problem does it solve? (CA in Hyperledger Fabric)

The Certificate Authority (CA) in Hyperledger Fabric solves identity management by issuing digital certificates to authenticate nodes and users, ensuring authorized access.
Hyperledger Fabric 中的证书颁发机构（CA）通过颁发数字证书解决身份管理问题，确保授权访问。

问题 65: What benefit does it bring? (Channel in Hyperledger Fabric)

Channels provide data privacy by isolating transactions and ledgers, ensuring only authorized channel members can access sensitive business data.
通道通过隔离交易和账本提供数据隐私，确保仅授权通道成员访问敏感商业数据。

问题 66: In Fabric, certificate authority is needed for identity management. Why is it important? Recall what’s man-in-the-middle attack?

Certificate Authority ensures trusted identities by issuing certificates, preventing man-in-the-middle attacks where attackers impersonate legitimate parties to intercept data.
证书颁发机构通过颁发证书确保可信身份，防止中间人攻击，即攻击者冒充合法方拦截数据。

问题 67: Do we need to worry a lot about Byzantine faults?

In Hyperledger Fabric, Byzantine faults are less concerning due to its permissioned nature with pre-approved nodes, though consensus like Raft addresses potential faults.
在 Hyperledger Fabric 中，因许可制特性与预批准节点，拜占庭故障不那么令人担忧，但 Raft 等共识仍应对潜在故障。

问题 68: What’s the other type of fault?

The other type is a crash fault, where a node fails or stops responding but does not act maliciously, unlike Byzantine faults.
另一种是崩溃故障，节点失败或停止响应，但不进行恶意行为，与拜占庭故障不同。

问题 69: What's Raft? Can it counteract Sybil attack?

Raft is a crash-fault-tolerant consensus algorithm in Hyperledger Fabric for ordering transactions. It doesn't counteract Sybil attacks, as Fabric's permissioned network prevents unauthorized identities.
Raft 是 Hyperledger Fabric 中用于交易排序的崩溃容错共识算法。它不直接对抗 Sybil 攻击，因 Fabric 的许可制网络阻止未授权身份。

问题 70: How does Raft ordering service work? At most how many failed nodes can it withstand?

Raft orders transactions via a leader-based consensus, tolerating up to (N-1)/2 failed nodes, where N is the total number of nodes.
Raft 通过基于领导者的共识排序交易，可容忍最多 (N-1)/2 个故障节点，N 为节点总数。

问题 71: Can Raft solve the Byzantine Generals Problem?

Raft cannot solve the Byzantine Generals Problem, as it assumes non-malicious crash faults, not malicious behavior.
Raft 无法解决拜占庭将军问题，因其假设非恶意的崩溃故障，而非恶意行为。

7. 区块链应用相关问题

问题 72: Are all of these volatile? (Payment tokens)

Not all payment tokens are volatile; cryptocurrencies like Bitcoin are volatile, but stablecoins like USDT, pegged to assets, maintain stable value.
并非所有支付代币都波动；比特币等加密货币波动大，但 USDT 等与资产挂钩的稳定币保持价值稳定。

问题 73: We can categorise the tokens issued through blockchain networks into different types. What are they?

Tokens include payment tokens (e.g., Bitcoin), utility tokens (e.g., governance), security tokens (investment assets), and non-fungible tokens (NFTs).
代币包括支付代币（例如比特币）、实用代币（例如治理）、证券代币（投资资产）和非同质化代币（NFT）。

问题 74: What are stablecoins?

Stablecoins are cryptocurrencies pegged to stable assets (e.g., USD, gold) to minimize price volatility, used in trading, payments, and DeFi (e.g., USDT, USDC).
稳定币是与稳定资产（例如美元、黄金）挂钩的加密货币，减少价格波动，用于交易、支付和 DeFi（例如 USDT、USDC）。

问题 75: What are the different types? What's its benefit?

Stablecoin types include fiat-backed (e.g., USDT), crypto-backed (e.g., DAI), and algorithmic (e.g., UST). Benefits are price stability, liquidity, and fast cross-border transactions.
稳定币类型包括法币支持（例如 USDT）、加密支持（例如 DAI）和算法型（例如 UST）。优点是价格稳定、流动性和快速跨境交易。

问题 76: What is the difference between NFT and other tokens like Bitcoin/Ether?

NFTs are unique, indivisible digital assets (e.g., art), while Bitcoin and Ether are fungible, interchangeable, and divisible tokens.
NFT 是独特、不可分割的数字资产（例如艺术品），而比特币和以太坊是可互换、可分割的同质化代币。

问题 77: What is so special about it?

NFTs are special for their uniqueness, verifiable blockchain ownership, and ability to represent digital or physical assets, enabling use cases like digital art and gaming.
NFT 的特殊之处在于其独特性、区块链上的可验证所有权以及代表数字或物理资产的能力，支持数字艺术和游戏等用例。

问题 78: What is an SFT (ERC-1155)?

SFT (Semi-Fungible Token, ERC-1155) is an Ethereum standard combining fungible and non-fungible properties, managing multiple token types in one contract (e.g., game items).
SFT（半同质化代币，ERC-1155）是以太坊标准，结合同质化和非同质化属性，在单一合约中管理多种代币类型（例如游戏道具）。

问题 79: What's its use case?

ERC-1155 is used in gaming (fungible currency and non-fungible items) and supply chains (fungible batches and unique assets).
ERC-1155 用于游戏（同质化货币和非同质化道具）和供应链（同质化批次和独特资产）。

问题 80: What is a rentable NFT (ERC-4907)?

A rentable NFT (ERC-4907) is an Ethereum standard allowing temporary transfer of NFT usage rights without transferring ownership, enabling rental markets.
可租用 NFT（ERC-4907）是以太坊标准，允许临时转移 NFT 使用权而不转移所有权，支持租赁市场。

问题 81: How does it help with the current landscape of NFTs?

ERC-4907 enhances NFT accessibility by allowing rentals (e.g., for gaming or virtual land), reducing costs and expanding use cases.
ERC-4907 通过允许租用 NFT（例如用于游戏或虚拟土地）增强可访问性，降低成本并扩展用例。

问题 82: Metaverse: the role of blockchain - data continuity; transaction.

Blockchain ensures data continuity (persistent identities and assets) and secure, transparent transactions in the metaverse.
区块链确保元宇宙中的数据连续性（持久身份和资产）和安全、透明的交易。