IS6200 期末考试问题整理与答案

1. 货币相关问题（PAGE 9）

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：

1. **交换媒介**：用于购买商品和服务。
2. **记账单位**：提供价值的标准衡量。
3. **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. They serve as a medium of exchange in some contexts and can be a store of value, but their high 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。它们在某些场景下可作为交换媒介和价值储存，但高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（PAGE 10, 11, 14, 15, 16）

问题 4: How do we secure our own accounts?

Bitcoin accounts are secured using public-private key cryptography. The private key, kept secret by the user, signs transactions to prove ownership. Losing the private key results in loss of access to 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. No single entity controls the ledger.

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。没有单一实体控制账本。

问题 6: How should we trust the ledger maintainer?

Trust in Bitcoin's ledger is achieved through Proof of Work (PoW) consensus. Miners compete to solve computational puzzles, making it costly to manipulate the ledger. The longest valid chain is trusted by the network.

比特币账本的信任通过工作量证明（PoW）共识机制实现。矿工竞争解决计算难题，操纵账本成本高昂。网络信任最长的有效链。

问题 7: How do we protect ourselves from attacks?

Bitcoin protects against attacks by making them costly via Proof of Work. Attackers need significant computational power (51% attack) to alter the blockchain, which is economically impractical due to high energy costs.

比特币通过工作量证明使攻击成本高昂来防御攻击。攻击者需巨大算力（51%攻击）才能更改区块链，但高能耗使其经济上不可行。

问题 8: How does this help privacy?

Bitcoin's public-private key system provides pseudonymity, not full anonymity. Transactions are linked to public keys (addresses), not 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，而非完全匿名。交易与公钥（地址）相关联，而非真实身份，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. The blockchain is fully transparent, with all transactions publicly visible. Pseudonymity protects user identities while maintaining open ledger access.

比特币的伪匿名性与透明性不冲突。区块链完全透明，所有交易公开可见。伪匿名性保护用户身份，同时保持账本开放访问。

问题 10: Why or why not?

Bitcoin balances privacy and transparency. Pseudonymous addresses protect user identities (privacy), while the public blockchain ensures all transactions are verifiable (transparency), achieving both without conflict.

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），而公开区块链确保所有交易可验证（透明性），两者无冲突。

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 still allowing public verification of transaction 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），同时仍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 sender, receiver, and amount.

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提供可选的屏蔽交易，隐藏发送者、接收者和金额。

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 add blocks to the blockchain, ensuring security 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来验证交易并添加区块到区块链，通过计算消耗确保安全。

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的计算。

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 with no prior chain to adjust difficulty.

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，没有之前的链来调整难度。

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 Bitcoin protocol, e.g., SegWit to increase block capacity.
2. **Layer 2 (Off-Chain)**: Building solutions like the Lightning Network to process transactions off-chain.

比特币的两种扩展解决方案是：

1. **第一层（链上）**：修改比特币协议，例如SegWit以增加区块容量。
2. **第二层（链下）**：构建如闪电网络的链下解决方案来处理交易。

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

SegWit (Segregated Witness) is a Bitcoin protocol upgrade that separates signature data from transaction data, increasing block capacity and fixing transaction malleability. It solves the problem of limited block size (1MB) and enables Layer 2 solutions like the Lightning Network.

SegWit（隔离见证）是比特币协议升级，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问题。它解决了区块大小限制（1MB）的问题，并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 while settling final balances on the blockchain.

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、低成本的链下交易，最终余额在区块链上结算。

问题 19: What's Taproot?

Taproot is a Bitcoin soft fork (2021) that enhances privacy and efficiency by introducing Schnorr signatures and MAST (Merkelized Abstract Syntax Trees), making complex transactions appear like regular ones.

Taproot是2021年的比特币软分叉，通过引入Schnorr签名和MAST（默克尔化抽象语法树）增强隐私和效率，使复杂交易看起来像普通交易。

3. 加密技术相关问题（PAGE 13）

问题 20: What is encryption?

Encryption is the process of converting plaintext into ciphertext using a key to protect data confidentiality, ensuring only authorized parties can access it.

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，确保只有授权方能访问。

问题 21: Symmetric vs. Asymmetric?

- **Symmetric Encryption**: Uses the same key for encryption and decryption (e.g., AES). It's fast but requires secure key sharing.
- **Asymmetric Encryption**: Uses a public key for encryption and a private key for decryption (e.g., RSA). It's slower but secure for key exchange.
- **对称加密**：使用相同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**：使用公钥加密，私钥解密（例如RSA），速度较慢但适合密钥交换。

问题 22: What is a hash function?

A hash function is a one-way mathematical function that maps input data to a fixed-size output (hash) to ensure data integrity. It's deterministic, collision-resistant, and irreversible.

哈希函数是一种单向数学函数，将输入数据映射到固定大小的输出（哈希），用于确保数据完整性。它具有确定性、抗碰撞性和不可逆性。

问题 23: Know some basic properties of cryptographic hash functions

Basic properties of cryptographic hash functions include:

1. **Deterministic**: Same input always produces the same hash.
2. **Collision Resistance**: Hard to find two inputs producing the same hash.
3. **Preimage Resistance**: Hard to reverse the hash to find the original input.

加密哈希函数的基本属性包括：

1. **确定性**：相同输入始终产生相同哈希。
2. **抗碰撞性**：难以找到两个输入产生相同哈希。
3. **原像抗性**：难以逆向哈希找到原始输入。

问题 24: What's its difference from encryption?

Hash functions are one-way, producing a fixed-size output to verify integrity, and are not reversible. Encryption is reversible, transforming data 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，使用密钥转换数据以保护机密性。

问题 25: 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 a message or transaction.

数字签名使用非对称加密（私钥签名，公钥验证）来确保消息或交易的真实性、完整性和不可否认性。

问题 26: How it works?

A digital signature works by:

1. Hashing the message to create a digest.
2. Signing the digest with the sender's private key.
3. Verifying the signature with the sender's public key to ensure the message is unchanged and authentic.

数字签名的工作原理是：

1. 对消息进行哈希生成摘要。
2. 用发送者的私钥对摘要签名。
3. 用发送者的公钥验证签名，确保消息未更改且真实。

问题 27: Why we need it? (or how is it better than our traditional wet ink signature?)

Digital signatures are needed for secure digital transactions. They are better than wet ink signatures because they provide cryptographic proof of authenticity, integrity, and non-repudiation, and are harder to forge.

数字签名用于安全的数字交易。它们优于传统湿墨签名，因为它们提供加密证明的真实性、完整性和不可否认性，且更难伪造。

4. 以太坊相关问题（PAGE 17, 18, 19, 20, 21）

问题 28: What's added in Ethereum such that it can achieve things that Bitcoin is incapable of?

Ethereum adds smart contracts, programmable code running on the blockchain 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，即在区块链上运行的图灵完备语言的可编程代码，支持复杂的应用（如DeFi和DAO），超越了比特币的支付功能。

问题 29: What new feature we need to go beyond payment only?

The new feature is smart contracts, which allow programmable, self-executing agreements on the blockchain, enabling applications like lending, voting, and token creation.

新功能是智能合约，允许在区块链上运行可编程、自动执行的协议，支持借贷、投票和代币创建等应用。

问题 30: How do we safeguard the network while adding this new feature?

Ethereum safeguards smart contracts using the Gas mechanism, which limits computational resources, prevents infinite loops, and charges fees to deter malicious code execution.

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，并收取费用以阻止恶意代码执行。

问题 31: 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. Ethereum uses Gas limits to terminate runaway programs.

不能，停机问题证明无法预测程序是否在有限时间内停止。以太坊使用Gas限制终止失控程序。

问题 32: 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.

比特币通过其脚本语言支持有限编程（例如多重签名交易），但不是图灵完备的，与以太坊的智能合约不同。

问题 33: 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 basic payment functions.

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，仅限于基本支付功能。

问题 34: What is the halting problem?

The halting problem is a theoretical computer science problem proving that no algorithm can determine whether any program will halt or run indefinitely for all inputs.

停机问题是理论计算机科学问题，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 35: 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 the allocated computational resources.

以太坊通过对智能合约执行设置Gas限制来处理停机问题，停止超出分配计算资源的程序。

问题 36: What's finality?

Finality is the assurance that a blockchain transaction is permanently confirmed and cannot be reversed, achieved through consensus mechanisms like PoW or PoS.

确定性是区块链交易被永久确认且不可逆的保证，通过如PoW或PoS的共识机制实现。

问题 37: How's finality different between PoW and PoS?

In PoW (e.g., Bitcoin), finality is probabilistic, requiring multiple confirmations (e.g., 6 blocks) to reduce reversal risk. In PoS (e.g., Ethereum post-Merge), finality is deterministic, achieved after a fixed number of validator attestations.

在PoW（如比特币）中，确定性是概率性的，需多个确认（例如6个区块）以降低逆转风险。在PoS（如合并后的以太坊）中，确定性是确定性的，在固定数量的验证者证明后实现。

问题 38: Recall that one may launch 34% attack in PoS. What are the attacks and how can we counteract such attacks?

In PoS, a 34% attack involves controlling one-third of validators to disrupt consensus (e.g., delay finality). Countermeasures include slashing (penalizing malicious validators' stakes) and social coordination to isolate attackers.

在PoS中，34%攻击涉及控制三分之一的验证者以干扰共识（例如延迟确定性）。对策包括削减（惩罚恶意验证者的质押）和社交协调以隔离攻击者。

问题 39: What is "optimistic rollup"?

Optimistic Rollup is a Layer 2 scaling solution for Ethereum that processes transactions off-chain, assuming they are valid, and posts compressed data on-chain. It uses fraud proofs to challenge invalid transactions.

乐观Rollup是以太坊的第二层扩展解决方案，链下处理交易，假设交易有效，并将压缩数据发布到链上。它使用欺诈证明来挑战无效交易。

问题 40: What does it mean by "optimistic" here?

"Optimistic" means transactions are assumed valid by default, processed off-chain, and only challenged via fraud proofs if disputes arise, reducing on-chain computation.

"乐观"指交易默认被假设为有效，在链下处理，仅在出现争议时通过欺诈证明挑战，减少链上计算。

问题 41: How can we guarantee the validity of transactions submitted via rollup?

Validity is guaranteed by fraud proofs. Anyone can challenge an invalid transaction within a dispute period. If proven invalid, the rollup reverts the transaction, ensuring correctness.

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，Rollup会撤销交易，确保正确性。

问题 42: What're the differences between rollup and the Lightning Network?

- **Rollup**: Layer 2 for Ethereum, processes general transactions off-chain (e.g., smart contracts), posts data on-chain, uses fraud proofs or ZK proofs.
- **Lightning Network**: Layer 2 for Bitcoin, focuses on payment channels for fast, low-cost transfers, settles only channel balances on-chain.
- **Rollup**：以太坊的第二层，链下处理通用交易（例如智能合约），将数据发布到链上，使用欺诈证明或零知识证明。
- **闪电网络**：比特币的第二层，专注于支付通道以实现快速、低成本转账，仅将通道余额结算到链上。

问题 43: What happened at that time? (The DAO Hack in 2016)

In 2016, The DAO, a decentralized organization on Ethereum, was hacked due to a reentrancy vulnerability, allowing an attacker to drain 3.6 million ETH ($50 million).

2016年，以太坊上的去中心化组织The DAO因重入漏洞被黑客攻击，攻击者窃取了360万ETH（约5000万美元）。

问题 44: How did it happen?

The DAO hack exploited a reentrancy vulnerability in its smart contract. The attacker repeatedly called a withdrawal function before the contract updated its balance, draining funds.

DAO黑客攻击利用了智能合约的重入漏洞。攻击者在合约更新余额前反复调用提款函数，耗尽资金。

问题 45: What is the vulnerability that results in the hack?

The vulnerability was reentrancy, where a malicious contract repeatedly calls back into the DAO's withdrawal function before the original call updates the balance, allowing multiple withdrawals.

漏洞是重入，恶意合约在原始调用更新余额前反复回调DAO的提款函数，允许多次提款。

问题 46: How could we solve it?

Reentrancy can be solved by:

1. Using a mutex (lock) to prevent reentrant calls.
2. Updating state (e.g., balance) before external calls.
3. Using checked functions like `transfer` instead of `call`.

重入问题可通过以下方式解决：

1. 使用互斥锁（mutex）防止重入调用。
2. 在外部调用前更新状态（例如余额）。
3. 使用检查函数如`transfer`而非`call`。

问题 47: What's the consequence to Ethereum?

The DAO hack led to a hard fork, splitting Ethereum into Ethereum (ETH, which reversed the hack) and Ethereum Classic (ETC, which preserved the original chain).

DAO黑客攻击导致硬分叉，将以太坊分裂为以太坊（ETH，撤销了黑客攻击）和以太坊经典（ETC，保留原始链）。

5. DAO相关问题（PAGE 22）

问题 48: 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（Decentralized Autonomous Organization），一种基于区块链、通过智能合约和社区投票治理、无中央权威的实体。

问题 49: What is the agency conflict? How does DAO mitigate this problem?

Agency conflict arises when agents (e.g., managers) prioritize their interests over principals (e.g., shareholders). DAOs mitigate this by using transparent smart contracts and community voting to align incentives and reduce centralized control.

代理冲突指代理人（例如管理者）优先考虑自身利益而非委托人（例如股东）。DAO通过透明的智能合约和社区投票减轻此问题， aligning incentives并减少集中控制。

问题 50: What are the new challenges?

New challenges for DAOs include:

1. **Governance Complexity**: Low voter participation or minority control.
2. **Security Risks**: Smart contract vulnerabilities (e.g., DAO hack).

3. **Legal Compliance**: Uncertain regulatory frameworks.

DAO的新挑战包括：

1. **治理复杂性**：投票参与度低或少数人控制。
2. **安全风险**：智能合约漏洞（例如DAO黑客攻击）。
3. **法律合规**：不确定的监管框架。

问题 51: What are some common voting approaches?

Common DAO voting approaches include:

1. **Token-Based Voting**: Votes weighted by token holdings.
2. **Quadratic Voting**: Votes cost quadratically to balance influence.
3. **Reputation-Based Voting**: Votes based on user reputation scores.

DAO常见的投票方式包括：

1. **基于代币的投票**：投票权重基于代币持有量。
2. **二次方投票**：投票成本呈二次方增长以平衡影响力。
3. **基于声誉的投票**：投票基于用户声誉分数。

问题 52: What's quadratic voting?

Quadratic voting is a voting system where the cost of votes increases quadratically (e.g., 1 vote costs 1 token, 2 votes cost 4 tokens), encouraging balanced participation and reducing dominance by wealthy voters.

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），鼓励平衡参与并减少富裕投票者的主导。

问题 53: Does it prevent Sybil attack?

Quadratic voting partially mitigates Sybil attacks by making it costly to create multiple identities, but it's not foolproof. Additional measures like identity verification are needed.

二次方投票通过增加创建多个身份的成本部分缓解Sybil攻击，但并非万无一失。需要额外的身份验证措施。

6. Hyperledger Fabric相关问题（PAGE 23, 25）

问题 54: Why are Bitcoin/Ethereum-like blockchains not ideal for most business applications?

Bitcoin and Ethereum are public, permissionless blockchains with slow transaction speeds, high costs, and public data, unsuitable for businesses needing privacy, speed, and regulatory compliance. Hyperledger Fabric, a permissioned blockchain, addresses these issues.

比特币和以太坊是公共、无许可区块链，交易速度慢、成本高、数据公开，不适合需要隐私、速度和监管合规的企业。Hyperledger Fabric作为许可制区块链解决了这些问题。

问题 55: 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 only authorized participants access the network.

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，确保只有授权的节点和用户能访问网络。

问题 56: What benefit does it bring? (Channel in Hyperledger Fabric)

Channels in Hyperledger Fabric provide data privacy by creating isolated sub-networks with separate ledgers, allowing only channel members to access transactions and data.

Hyperledger Fabric中的通道通过创建隔离的子网络和独立账本提供数据隐私，仅允许通道成员访问交易和数据。

问题 57: Do we need to worry a lot about Byzantine faults?

In Hyperledger Fabric, Byzantine faults (malicious behavior) are less concerning than in public blockchains due to its permissioned nature, where trusted nodes are pre-approved. However, consensus mechanisms like Raft still address potential faults.

在Hyperledger Fabric中，由于其许可制特性，预先批准的可信节点使得拜占庭故障（恶意行为）不那么令人担忧。然而，Raft等共识机制仍可应对潜在故障。

问题 58: What's the other type of fault?

The other type of fault is a crash fault, where a node fails or stops responding but does not act maliciously, unlike Byzantine faults.

另一种故障是崩溃故障，即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 59: What's Raft? Can it counteract Sybil attack?

Raft is a crash-fault-tolerant consensus algorithm used 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，因为Fabric的许可制网络阻止未授权身份。

7. 区块链应用相关问题（PAGE 26, 27）

问题 60: Are all of these volatile? (Payment tokens)

Not all payment tokens are volatile. Cryptocurrencies like Bitcoin and Ether are volatile, but stablecoins like USDT, pegged to assets like the USD, maintain stable value.

并非所有支付代币都波动。比特币和以太坊等加密货币波动大，但像USDT这样与美元等资产挂钩的稳定币保持价值稳定。

问题 61: What are stablecoins?

Stablecoins are cryptocurrencies pegged to stable assets (e.g., USD, gold) to minimize price volatility, used for 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，以最小化价格波动，用于交易、支付和DeFi（例如USDT、USDC）。

问题 62: What are the benefits of stablecoins?

Benefits of stablecoins include:

1. **Price Stability**: Pegged to assets like USD, reducing volatility.

2. **Liquidity**: Widely used in trading and DeFi.
3. **Fast Transactions**: Enable low-cost, cross-border payments.

稳定币的优点包括：

1. **价格稳定**：与美元等资产挂钩，减少波动。
2. **流动性**：在交易和DeFi中广泛使用。
3. **快速交易**：支持低成本、跨境支付。

问题 63: What is the difference between NFT and other tokens like Bitcoin/Ether?

NFTs (Non-Fungible Tokens) are unique, indivisible digital assets (e.g., art, collectibles), while Bitcoin and Ether are fungible tokens, interchangeable and divisible.

NFT（非同质化代币）是独特、不可分割的数字资产（例如艺术品、收藏品），而比特币和以太坊是可互换、可分割的同质化代币。

问题 64: What is so special about it?

NFTs are special due to their uniqueness, verifiable ownership on the blockchain, and ability to represent digital or physical assets, enabling new 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新用例。

问题 65: What is an SFT (ERC-1155)?

SFT (Semi-Fungible Token, ERC-1155) is a token standard on Ethereum that combines fungible and non-fungible properties, allowing a single contract to manage multiple token types (e.g., game items).

SFT（半同质化代币，ERC-1155）是以太坊上的代币标准，结合同质化和非同质化属性，允许单一合约管理多种代币类型（例如游戏道具）。

问题 66: What's its use case?

ERC-1155's use cases include gaming (managing fungible in-game currency and non-fungible unique items) and supply chain (tracking fungible batches and unique assets).

ERC-1155的用例包括游戏（管理同质化的游戏货币和非同质化的独特道具）和供应链（跟踪同质化批次和独特资产）。

问题 67: What is a rentable NFT (ERC-4907)?

A rentable NFT (ERC-4907) is an Ethereum token standard that allows temporary transfer of NFT usage rights without transferring ownership, enabling rental markets for digital assets.

可租用NFT（ERC-4907）是以太坊代币标准，允许临时转移NFT使用权而不转移所有权，支持数字资产的租赁市场。

问题 68: How does it help with the current landscape of NFTs?

ERC-4907 enhances NFT accessibility by allowing users to rent NFTs (e.g., for gaming or virtual land) without buying, reducing costs and expanding use cases.

ERC-4907通过允许用户租用NFT（例如用于游戏或虚拟土地）而无需购买，降低成本并扩展用例，增强NFT的可访问性。