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.

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.

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.

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.

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.

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.

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.

问题 8: How does this help privacy?

Bitcoin's public-private key system provides pseudonymity(伪匿名性), linking transactions to addresses rather than real identities, offering some privacy unless linked to personal information.

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.

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

问题 27: How digital signature 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

问题 37: What’s finality? 永久确认且不可逆的保证，通过共识机制实现。

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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`.

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).

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.

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.

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.

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.

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.

问题 55: What is the agency conflict?

Agency conflict arises when agents favor their interests over principals.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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(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.

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.

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.

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, other nodes sync with the leader, tolerating up to (N-1)/2 failed nodes, where N is the total number of nodes.

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.

7. 区块链应用相关问题

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

Not all payment tokens are volatile; cryptocurrencies like Bitcoin are volatile, but stablecoins like USDT, pegged to assets, maintain stable value.

问题 73: We can categorise the token into different types?

Tokens include payment tokens (e.g., Bitcoin), utility tokens (e.g., governance), security tokens (investment assets), and non-fungible tokens (NFTs).

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).

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）。

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.

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.

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).

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).

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.

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.