技术类（16-19）

面试问答题（中英文）

技术类（16-19）

16、你了解哪些去中心化存储解决方案?

What decentralized storage solutions do you know?

答:

1.IPFS：特点是内容寻址的文件存储和共享协议。优点是高效分发、数据冗余、抗审查。

2.Filecoin:特点是基于IPFS的存储网络，有经济激励机制。优点是长期存储保障，通过市场机制激励存储提供者。

3.Storj:特点是利用空闲硬盘空间提供云存储服务。优点是数据加密、安全性高、分布式存储。

4.Sia:特点是租用其他用户的硬盘空间进行存储。优点是低成本、高安全性，利用智能合约确保可靠性。

5.Arweave:特点是永久存储协议。优点是一次性付费，永久存储，适合存档和数据持久保存。

6.Swarm:特点是以太坊生态系统的存储解决方案。优点是与以太坊深度集成，支持去中心化应用的数据存储。

1.IPFS: Characterized as a content-addressed file storage and sharing protocol. Benefits include efficient distribution, data redundancy, and censorship resistance.

2.Filecoin: features an IPFS-based storage network with economic incentives. Advantages are long-term storage guarantees and incentives for storage providers through market mechanisms.

3.Storj: characterized by the use of free hard disk space to provide cloud storage services. Advantages are data encryption, high security, distributed storage.

4.Sia: Characterized by renting other users' hard disk space for storage. Advantages are low cost, high security, and the use of smart contracts to ensure reliability.

5.Arweave:Features permanent storage agreement. Advantages are one-time payment, permanent storage, suitable for archiving and data persistence.

6.Swarm:Features a storage solution for the Ethernet ecosystem. Benefits are deep integration with Ether and support for data storage for decentralized applications.

17、什么是DAO？它们是如何运作的？

What are DAOs and how do they work?

答：

DAO特点是去中心化，自治和透明性。去中心化就是没有中心化的管理层，所有决策由社区成员投票决定。自治就是运营规则和决策流程由智能合约预先设定，并自动执行。透明性就是所有交易和决策记录在区块链上，是公开透明的。

DAO的运作方式是由智能合约定义和执行DAO的规则和决策。成员通过持有代币获得投票权。成员提出提案并投票决定，智能合约自动执行通过的提案。DAO的资金池由智能合约管理，使用需成员投票批准。

DAO应用于投资基金，去中心化金融（DeFi），社区治理和公共资源管理。优势是透明性，参与性，效率高。透明性是决策和资金流动公开。参与性是成员广泛参与提案和投票。效率高是自动执行决策。挑战是安全性不够，智能合约漏洞风险，而且法律地位不明确，有效管理和决策具有挑战。

DAO通过去中心化的方式实现了自治管理，具有透明、高效和参与性强的特点，广泛应用于投资、DeFi和社区治理等领域。

DAOs are characterized by decentralization, autonomy and transparency. Decentralization means that there is no centralized management and all decisions are voted by community members. Autonomy means that the operating rules and decision-making processes are pre-set by smart contracts and executed automatically. Transparency means that all transactions and decisions are recorded on the blockchain and are open and transparent.

DAO operates in a way that the rules and decisions of DAO are defined and executed by smart contracts. Members gain voting rights by holding tokens. Members make proposals and vote on them, and the smart contract automatically executes the passed proposals. The DAO's pool of funds is managed by the smart contract, and its use needs to be approved by members' votes.

DAO is used in investment funds, decentralized finance (DeFi), community governance and public resource management. The advantages are transparency, participation and efficiency. Transparency is the openness of decision-making and financial flows. Participation is the extensive involvement of members in proposing and voting. Efficiency is automated decision making. Challenges are insufficient security, risk of smart contract vulnerabilities, and unclear legal status, making effective management and decision-making challenging.

DAO achieves self-governance through decentralization, is transparent, efficient and participatory, and is widely used in areas such as investment, DeFi and community governance.

18、如何在区块链上进行身份验证?

How to authenticate on blockchain?

答：

1.去中心化身份（DID）

原理是用户生成公私钥对，创建唯一的DID，注册在区块链上。用户用私钥签名信息证明身份，应用于Sovrin、uPort。

2.数字证书和区块链

原理是认证机构颁发数字证书，哈希值记录在区块链上。通过区块链确认证书真实性，应用于Blockcerts。

3.零知识证明（ZKP）

原理是用户生成零知识证明，证明身份属性。验证者验证证明有效性而不获取具体身份信息，应用于Zcash、zk-SNARKs。

4.代币和访问控制

原理是使用代币或智能合约控制资源访问。用户通过身份验证后获得代币，使用代币访问资源，应用于ERC-725、ERC-735。

1.Decentralized Identity (DID)

The principle is that the user generates a public-private key pair to create a unique DID, which is registered on blockchain. Users use the private key to sign information to prove their identity, applied to Sovrin, uPort.

2.Digital certificate and blockchain

The principle is that the certification authority issues a digital certificate and the hash value is recorded on blockchain. The authenticity of the certificate is confirmed through the blockchain, which is used in Blockcerts.

3.Zero Knowledge Proof (ZKP)

The principle is that the user generates zero-knowledge proof to prove identity attributes. The verifier verifies the validity of the proof without obtaining specific identity information, applied to Zcash, zk-SNARKs.

4.Token and Access Control

The principle is to use tokens or smart contracts to control access to resources. Users obtain tokens after authentication and use them to access resources, applied in ERC-725, ERC-735.

19、你对Web3中的隐私保护有什么看法?

What are your thoughts on privacy protection in Web3?

答:

1.零知识证明（ZKP）的原理是在不泄露具体数据的情况下，证明某一声明的真实性。应用在Zcash中使用zk-SNARKs保护交易隐私。

2.环签名（Ring Signatures）的原理是一组用户共同签署交易，使外界无法确定具体签名者，应用于Monero提高交易隐私性。

3.隐私智能合约的原理是使用加密技术隐藏合约内容和参与者信息，应用于Enigma、Secret Network。

4.混币服务（Mixing Services）的原理是混合多笔交易，模糊交易来源和去向。应用于Wasabi Wallet、CoinJoin。

5.去中心化身份（DID）的原理是用户控制自己的身份信息，仅在必要时共享数据，应用于Sovrin、uPort。

6.同态加密（Homomorphic Encryption）的原理是在加密数据上进行计算，保护数据隐私，未来可能用于隐私保护的智能合约。

1.Zero Knowledge Proof (ZKP) works on the principle of proving the truthfulness of a statement without revealing specific data. Applications use zk-SNARKs in Zcash to protect transaction privacy.

2.The principle of Ring Signatures is that a group of users co-sign a transaction, so that the outside world can not determine the specific signer, which is used in Monero to improve transaction privacy.

3.The principle of privacy smart contracts is to use encryption technology to hide the content of the contract and participant information, applied to Enigma, Secret Network.

4.The principle of Mixing Services is to mix multiple transactions, blurring the origin and destination of transactions. Used in Wasabi Wallet, CoinJoin.

5.The principle of Decentralized Identity (DID) is that users control their own identity information and share data only when necessary, applied in Sovrin, uPort.

6.Homomorphic Encryption (Homomorphic Encryption) is based on the principle of computing on encrypted data to protect data privacy, and may be used for privacy-protecting smart contracts in the future.