技术实现类16-20

面试问答

技术实现类Technology Realization Category（16-20）

16、ERC777 代币存在什么危险?

What are the dangers of ERC777 tokens?

答:

ERC777 代币是一种功能型代币，它在 ERC20 标准的基础上进行了改进，解决了一些 ERC20 标准存在的问题。ERC777 代币的主要优势是它支持发送代币时携带额外的信息，同时也支持代币的操作员功能。此外，ERC777 代币还可以通过 ERC1820 接口注册表合约来实现代币转账的监听，增强了代币的安全性.虽然 ERC777 代币有很多优点，但是它也存在一些潜在的危险。由于 ERC777 代币是一种相对较新的代币标准，因此它的生态系统相对较小，可能存在一些安全漏洞。此外，ERC777 代币的操作员功能也可能会被滥用，导致代币被盗或者其他安全问题。因此，在使用 ERC777 代币时，需要谨慎选择代币合约，同时也需要注意代币的安全性.

The ERC777 Token is a functional token that improves on the ERC20 standard by addressing some of the problems of the ERC20 standard.The main advantage of the ERC777 Token is that it supports the ability to send tokens with additional information, as well as support for token operator functions. In addition, ERC777 tokens can listen to token transfers through the ERC1820 interface registry contract, which enhances the security of tokens.

Although the ERC777 token has many advantages, it also has some potential dangers. Since the ERC777 token is a relatively new token standard, it has a relatively small ecosystem and may have some security vulnerabilities. In addition, the operator function of ERC777 tokens can be abused, leading to token theft or other security issues. Therefore, when using ERC777 tokens, you need to choose the token contract carefully and also pay attention to the security of the tokens.

17、OpenZeppelin ERC721 实现中的 safeMint 与 mint 有何不同?

What is the difference between safeMint and mint in the OpenZeppelin ERC721 implementation?

答：

在OpenZeppelin ERC721实现中，safeMint和mint都是用于创建新的ERC721代币的函数，但它们之间有一些区别。mint函数只是简单地创建一个新的ERC721代币，并将其分配给指定的地址。而safeMint函数则会在创建新的ERC721代币之前检查目标地址是否支持ERC721转移。如果目标地址不支持ERC721转移，则safeMint函数会抛出异常并阻止创建新的ERC721代币。因此，safeMint函数比mint函数更安全，因为它可以防止ERC721代币被锁定在不支持ERC721转移的合约中。

In the OpenZeppelin ERC721 implementation, both safeMint and mint are functions used to create new ERC721 tokens, but there are some differences between them. Mint function simply creates a new ERC721 token and assigns it to the specified address. The safeMint function, on the other hand, checks if the target address supports ERC721 transfers before creating a new ERC721 token. If the target address does not support ERC721 transfers, the safeMint function throws an exception and prevents the creation of new ERC721 tokens. Therefore, the safeMint function is safer than the mint function because it prevents ERC721 tokens from being locked in contracts that do not support ERC721 transfers.

18、ERC165 作用于什么?

What does ERC165 do?

答：

ERC165是一个标准，用于检测和发布智能合约实现的接口。它标准化了如何识别接口，如何检测它们是否实现了ERC165或其他接口，以及合约将如何发布它们实现的接口。它可以帮助您查询合约实现的特定接口，以及更重要的是，该智能合约实现的版本。

ERC165 is a standard for detecting and publishing interfaces implemented by smart contracts. It standardizes how interfaces are identified, how to detect if they implement ERC165 or other interfaces, and how contracts will publish the interfaces they implement. It helps you to query the specific interface that a contract implements and, more importantly, the version of that smart contract implementation.

19、ERC721A如何减少铸造成本?有什么权衡?

How does ERC721A reduce casting costs? What are the tradeoffs?

答：

ERC721A是一个改进的ERC721标准，旨在通过减少铸造成本来提高NFT的可扩展性。ERC721A通过引入批量铸造API来实现这一点，从而将铸造成本降低到O(1)的时间复杂度。与OZ的单独铸造方式不

同，ERC721A的批量铸造API可以同时铸造多个NFT，而不需要循环调用单独的铸造方法。这种方法可以显著减少铸造成本，但需要权衡的是，它可能会降低NFT的安全性。

ERC721A is an improved ERC721 standard designed to improve the scalability of NFTs by reducing casting costs.ERC721A accomplishes this by introducing a batch casting API that reduces casting costs to O(1) time complexity. Unlike OZ's individual casting approach, ERC721A's batch casting API allows for the simultaneous casting of multiple NFTs without the need for cyclic calls to individual casting methods. This approach can significantly reduce casting costs, but the tradeoff is that it may reduce the security of the NFTs.

20、Compound Finance 如何计算利用率?

How does Compound Finance calculate utilization rates?

答:

Compound Finance 是一个算法化的、自治的利率协议，旨在为开发者解锁一系列开放式金融应用。该协议的利用率是指借款人从 Compound 借入资产的数量与抵押品价值的比率。具体地，它是通过将所有借款人的借款总额除以所有抵押品的总价值来计算的。这个比率越高，代表 Compound 的借款人越多，市场上的资金也越紧张。（从compound中借款，可通过增加抵押品价值降低借款利率）。

Compound Finance is an algorithmic, autonomous rate protocol designed to unlock a range of open finance applications for developers. The protocol's utilization rate is the ratio of the amount of assets a borrower borrows from Compound to the value of the collateral. Specifically, it is calculated by dividing the total amount borrowed by all borrowers by the total value of all collateral. The higher this ratio, the more borrowers Compound has and the tighter the market is. (Borrowing from Compound reduces the borrowing rate by increasing the value of the collateral.)