实践经验类(1-5)

面试问答题（中英文）

实践经验类 Practical experience category（1-5）

1、什么是签名重放攻击?

What is Signature Replay Attack?

答:

签名重放攻击是一种网络攻击，攻击者通过重复使用已经被验证的数字签名来欺骗系统。数字签名是一种用于验证数据完整性和身份验证的技术，它使用公钥密码学来生成和验证签名。在签名重放攻击中，攻击者截获了一个数字签名并将其重复使用，以便在未经授权的情况下执行某些操作。例如，攻击者可以使用重放攻击来多次执行某个交易，从而导致资金损失。

为了防止签名重放攻击，您可以使用以下方法:

使用时间戳或随机数来确保每个数字签名只能使用一次。

使用序列号来确保数字签名按顺序使用。

使用加密协议来保护数字签名，例如TLS或SSL。

A signature replay attack is a network attack in which an attacker spoofs a system by reusing digital signatures that have already been verified. Digital signature is a technique used to verify data integrity and authentication, which uses public key cryptography to generate and verify signatures. In a signature replay attack, an attacker intercepts a digital signature and reuses it to perform certain actions without authorization. For example, an attacker could use a replay attack to execute a transaction multiple times, resulting in a loss of funds.

To prevent signature replay attacks, you can use the following methods:

Use timestamps or random numbers to ensure that each digital signature can be used only once.

Use serial numbers to ensure that digital signatures are used sequentially.

Use a cryptographic protocol to protect digital signatures, such as TLS or SSL.

2、描述三种存储 gas 成本类型。

Describe the three storage gas cost types.

答：

1.内存变量：内存变量是指在函数执行期间分配的临时变量。它们的gas成本取决于它们的大小，通常比存储变量更便宜。在函数执行结束后，内存变量将被销毁。

2.存储变量：存储变量是指在合约存储器中永久存储的变量。它们的gas成本取决于它们的大小，通常比内存变量更昂贵。存储变量的gas成本还取决于它们的位置，例如，如果它们位于映射中，则访问映射中的元素的成本更高。

3.状态变量：状态变量是指在合约存储器中永久存储的变量，但它们是在合约创建时定义的。与存储变量相比，它们的gas成本更便宜，因为它们只需要在合约创建时初始化一次。

1.Memory variables: Memory variables are temporary variables allocated during function execution. Their gas cost depends on their size and are usually cheaper than memory variables. At the end of function execution, memory variables are destroyed.

2.Stored variables: Stored variables are variables that are permanently stored in contract memory. Their gas cost depends on their size and is usually more expensive than memory variables. The gas cost of stored variables also depends on their location, e.g., if they are located in a mapping, it is more expensive to access the elements of the mapping.

3.State variables: State variables are variables that are permanently stored in the contract memory, but they are defined when the contract is created. They have a cheaper gas cost compared to stored variables because they only need to be initialized once at contract creation time.

3、为什么构造函数不应该使用在可升级合约里?

Why should constructors not be used in scalable contracts?

答：

使用构造函数来初始化合约状态变量是一种常见的做法，但是这会导致合约的状态变量无法升级。因为在升级合约时，新的合约代码将会被部署到一个新的地址，而旧的合约状态变量将无法被传递到新的合约中。因此，为了使合约状态变量能够升级，应该使用初始化函数来初始化合约状态变量，而不是构造函数。初始化函数可以在合约部署后随时调用，因此可以在升级合约时重新初始化合约状态变量。

It is common practice to use constructors to initialize contract state variables, but this makes it impossible to upgrade a contract's state variables. This is because when upgrading a contract, the new contract code will be deployed to a new address and the old contract state variables will not be able to be passed to the new contract. Therefore, in order to enable contract state variables to be upgraded, an initialization function should be used to initialize the contract state variables instead of a constructor. The initialization function can be called anytime after the contract has been deployed, so it is possible to reinitialize the contract state variables when upgrading the contract.

4、如果合约通过 delegate call 调用一个空地址或之前已自毁的合约，会发生什么？如果是常规调用而不是 delegatecall 会发生什么？

What happens if a contract calls a null address or a previously self-destructed contract via delegatecall? What happens if it is a regular call instead of a delegate call?

答：

如果合约通过delegatecall调用一个空地址或之前已自毁的合约，会导致delegatecall返回false，并且不会发生任何状态更改。如果是常规调用而不是delegatecall，则会导致交易失败并回滚，因为您不能调用一个不存在的合约或已自毁的合约。

If a contract calls a null address or a previously self-destructed contract via delegatecall, this causes delegatecall to return false and no state change occurs. A regular call instead of a delegate call will cause the transaction to fail and be rolled back because you cannot call a non-existent or self-destructing contract.

5、如果向一个会回滚的函数进行 delegate call，delegate call 会怎么做？

What does a delegate call do if it is made to a function that rolls back?

答：

如果向一个会回滚的函数进行 delegate call，delegate call 会返回 false，并且不会发生任何状态更改。如果是常规调用而不是 delegate call，则会导致交易失败并回滚，因为您不能调用一个不存在的合约或已自毁的合约。

If you make a delegate call to a function that rolls back, the delegate call returns false and no state changes occur. If it's a regular call instead of a delegate call, the transaction fails and rolls back because you can't call a non-existing contract or a self-destructing contract.