

Certainly! Let's walk through each of these Solidity topics in depth, complete with theory, detailed definitions, and annotated `pragma solidity` code examples. I'll structure them clearly so they're easy to study for your exams. Let me know if you'd like any part expanded further!

1. Visibility and Activity Qualifiers (Function and State Variable Visibility)

Solidity uses **visibility specifiers** to control access to functions and state variables, and **mutability/activity qualifiers** to specify what operations a function can perform.

Visibility Specifiers

- **public**: Accessible internally (within contract and derived contracts), externally (via transactions or call).
- **external**: Only callable from outside the contract (but `this.func()` from inside is allowed).
- **internal**: Only accessible within the contract and derived contracts.
- **private**: Only accessible within the contract defining it.

Mutability Specifiers (Activity Qualifiers)

- **pure**: Neither reads nor modifies state.
- **view**: Reads state but does not modify it.
- **(no specifier)**: Can read and modify state (default).
- **payable**: Allows the function to receive Ether.

Example:

```
pragma solidity ^0.8.0;

contract VisibilityActivity {
    uint private _privateVar = 1;
    uint internal _internalVar = 2;
    uint public publicVar = 3;

    function getPrivate() external view returns (uint) {
        return _privateVar; // external->public via this function
    }

    function incrementInternal() internal {
        _internalVar += 1;
    }

    function doIncrement() public {
        incrementInternal();
    }

    function readPublicVar() public view returns (uint) {
        return publicVar;
    }

    function pureFunction(uint x) public pure returns (uint) {
        return x * 2; // doesn't read or write state
    }

    receive() external payable { /* Accept ETH */ }

    function deposit() external payable {
```

```
    // payable function; can receive Ether
  }
}
```

2. `address` and `address payable`

- **`address`**: Stores a 20-byte Ethereum address. Cannot receive Ether by default.
- **`address payable`**: Extends `address` with `.transfer()`, `.send()`, `.call{value: ...}()` for sending Ether.

Example:

```
pragma solidity ^0.8.0;

contract AddressTypes {
    address public normalAddress;
    address payable public payableAddress;

    constructor(address payable _payable) {
        normalAddress = msg.sender;
        payableAddress = _payable;
    }

    function sendEtherViaTransfer() external payable {
        payableAddress.transfer(msg.value); // only payable addresses
    }

    function sendEtherViaCall() external payable {
        (bool success, ) = payableAddress.call{value: msg.value}("");
        require(success, "Transfer failed");
    }
}
```

3. `bytes` Types and `enum`

`bytes`

- **`bytes`**: Dynamically-sized byte array (`bytes[]`). Useful for raw data.
- **`bytes1–bytes32`**: Statically-sized byte arrays.

`enum`

Defines custom types with fixed set of values.

Example:

```
pragma solidity ^0.8.0;

contract BytesEnums {
    bytes public dynamicData = "Hello";
    bytes32 public fixedData = "HelloFixedLength.....";
    bytes1 public singleByte = 0xFF;

    enum State { Created, Locked, Inactive }
    State public contractState;

    function setState(State _state) public {
        contractState = _state;
    }
}
```

```
}
```

4. Arrays: Fixed and Dynamic

- **Fixed-size arrays:** Defined with a constant length (e.g., `uint[5]`).
- **Dynamic arrays:** Size can change (e.g., `uint[]`).

Example:

```
pragma solidity ^0.8.0;

contract ArraysDemo {
    uint[3] public fixedArr;
    uint[] public dynamicArr;

    constructor() {
        fixedArr = [1, 2, 3];
        dynamicArr.push(10);
        dynamicArr.push(20);
    }

    function updateFixed(uint index, uint value) public {
        fixedArr[index] = value;
    }

    function addToDynamic(uint value) public {
        dynamicArr.push(value);
    }

    function popFromDynamic() public {
        dynamicArr.pop();
    }

    function getDynamicLength() public view returns (uint) {
        return dynamicArr.length;
    }
}
```

5. Special Arrays: `bytes` and `string`

`bytes` (dynamic): Work similarly to `uint8[]` but optimized. `string` is also dynamic, but for UTF-8 text.

```
pragma solidity ^0.8.0;

contract SpecialArrays {
    bytes public dataBytes;
    string public dataString;

    function setBytes(bytes calldata newData) external {
        dataBytes = newData;
    }

    function setString(string calldata newString) external {
        dataString = newString;
    }

    function getByteAt(uint idx) external view returns (byte) {
        return dataBytes[idx];
    }
}
```

6. struct

Custom complex data types.

```
pragma solidity ^0.8.0;

contract StructDemo {
    struct Person {
        string name;
        uint age;
    }

    Person[] public people;

    function addPerson(string calldata name, uint age) external {
        people.push(Person(name, age));
    }

    function getPerson(uint idx) external view returns (string memory, uint) {
        Person storage p = people[idx];
        return (p.name, p.age);
    }
}
```

7. mapping

Associative arrays (hash tables) — no enumeration.

```
pragma solidity ^0.8.0;

contract MappingDemo {
    mapping(address => uint) public balances;
    mapping(uint => Person) public peopleById;

    struct Person {
        string name;
        uint age;
    }

    uint public nextId;

    function deposit() external payable {
        balances[msg.sender] += msg.value;
    }

    function addPerson(string calldata name, uint age) external {
        peopleById[nextId] = Person(name, age);
        nextId++;
    }

    function getBalance(address user) external view returns (uint) {
        return balances[user];
    }
}
```

8. Inheritance

Contracts can inherit from parent contracts, combining features and overriding behaviors.

```
pragma solidity ^0.8.0;
```

```

contract Base {
    event Log(string message);

    function sayHello() public virtual {
        emit Log("Hello from Base");
    }
}

contract Derived is Base {
    function sayHello() public override {
        emit Log("Hello from Derived");
    }
}

```

You can also use multiple inheritance:

```

contract A { function foo() public virtual { } }
contract B { function bar() public virtual { } }
contract C is A, B {
    function foo() public override(A) { super.foo(); }
    function bar() public override(B) { super.bar(); }
}

```

9. Error Handling: `require`, `revert`, `assert`, `try/catch`

- **`require(condition, "message")`**: Validates inputs or external calls; refunds unused gas.
- **`revert("message")`**: Same as `require`, for when wanting to revert explicitly.
- **`assert(condition)`**: Checks for invariants; should not fail (used for internal errors).
- **`try/catch`**: Handling errors from external contract calls or contract creation.

```

pragma solidity ^0.8.0;

interface ICounter {
    function inc() external returns (uint);
}

contract ErrorHandling {
    uint public count = 0;

    function safeInc(ICounter counter) external {
        try counter.inc() returns (uint newCount) {
            count = newCount;
        } catch Error(string memory reason) {
            // revert with the reason
            revert(reason);
        } catch (bytes memory /*lowLevelData*/) {
            revert("Low-level failure");
        }
    }

    function checkPositive(int x) public pure {
        require(x >= 0, "Negative not allowed");
    }

    function invariant(uint x) public pure {
        assert(x < 100); // Should always hold true
    }
}

```

Summary Table

Topic	Purpose
Visibility & Activity	Control access and state-read/write capabilities
address vs address payable	Store addresses; payable allows Ether transfers
bytes & enum	Raw data (fixed/dynamic) and custom options
Arrays (fixed/dynamic)	Lists of elements (with constant or variable length)
Special arrays (bytes, string)	Raw binary and text handling
struct	Custom composite data types
mapping	Key-value storage without enumeration
Inheritance	Share and override functionality across contracts
Error handling	Validate conditions and manage exceptions

Let me know any specific topic you'd like deeper examples on—like advanced inheritance, memory vs storage, `abi.encode`, or best practices for error handling. Good luck with your exam prep!

Great observation! The underscore (`_`) prefix in variable names like `_payable` or `_internalVar` is **not required** by Solidity — it's a **naming convention** commonly used by developers to distinguish between:

✓ Purpose of Using an Underscore (`_`) in Variable Names

1. To distinguish function parameters from state variables
2. To signal private/internal use (not enforced by Solidity)
3. To improve code readability and avoid naming conflicts

🔍 Example 1: Function Parameter vs. State Variable

```
pragma solidity ^0.8.0;

contract Example {
    uint public value;

    // Without underscore: potential conflict
    function setValue(uint value) public {
        value = value; // This doesn't work! It assigns the parameter to itself.
    }

    // With underscore: clear intent
    function setValueFixed(uint _value) public {
        value = _value; // Now, we're assigning the parameter to the state variable
    }
}
```

💡 The underscore helps to differentiate between `value` (state variable) and `_value` (function parameter).

🔍 Example 2: Internal or Private Variables

```
pragma solidity ^0.8.0;

contract Bank {
    uint internal _balance;

    function deposit(uint amount) public {
        _balance += amount;
    }

    function getBalance() public view returns (uint) {
        return _balance;
    }
}
```

Here, `_balance` is used to indicate it's an **internal** variable — just a developer-friendly hint.

Example 3: Constructor Parameter Naming

```
pragma solidity ^0.8.0;

contract Owner {
    address public owner;

    constructor(address _owner) {
        owner = _owner; // Assigning constructor parameter to state variable
    }
}
```

Without the underscore, you'd have a name collision (e.g., `owner = owner;`) — the compiler wouldn't know whether you mean the parameter or the state variable.

Summary

Usage

Function parameters To distinguish from state variables with same name

Internal/private vars Just a convention to show "internal use"

Readability Makes code more understandable, especially in large contracts

Why Use Underscore _?

Important Note:

Solidity does **not require** underscores. It's **just a developer naming convention** — similar to how private variables in Python are named with a `_` prefix.

You can choose your own style, but following this convention helps maintain **readable, bug-free code** — especially in teams or open-source projects.

Let me know if you want help setting up naming conventions for your own smart contracts!