Solidity汇编应用案例

- 字节码
  - creationCode
    - type(ContractName).creationCode
    - 合约部署时，需要构造函数结构及参数
      - 产生了一笔交易，其中data数据是 creationCode+abi.encode(constructor参数)
  - runtimeCode
    - type(ContractName).runtimeCode
    - 调用合约时，产生了一笔交易，其中data数据是 callldata
- bytecode的bytes结构
  - 前32字节存bytes的长度
  - 后面是内容
- create/create2
  - create
    - 默认合约创建方式
    - creata(value,offset,length)
      - addr = new memory[offset:offset+length].value(value)
  - creata2(value,offset,length,salt)
    - 可提前计算合约地址
    - bytecode = creationCode+abi.encode(constructor参数)
    - addr := create2(callvalue(),add(bytecode, 0x20),mload(bytecode), _salt)
  - extcodesize(addr)
    - 返回 address(addr).code.size
    - 为runtimeCode的字节大小
- getAddress（非汇编）
  - bytecode = creationCode+abi.encode(constructor参数)
  - bytes32 hash = keccak256(abi.encodePacked(bytes1(0xff), address(this), _salt, keccak256(bytecode)));
  - 地址：address(uint160(uint256(hash)))
- Minimal Proxy
  - proxy合约的汇编代码最简化
  - 通过copy一个合约的abi方法，实现多个最小代理