

# 第七课作业

## 搭建智能合约环境与测试

```
root@51db756e5aa7:/src/blockstack-core/sample# clarity-cli generate_address
SP23FEK5XGYT79HKZEDUHF548NYU33FSA3C1QBSM4
root@51db756e5aa7:/src/blockstack-core/sample# clarity-cli initialize /data/db
Database created.
root@51db756e5aa7:/src/blockstack-core/sample# ls
helloworld.clar  sum.clar
root@51db756e5aa7:/src/blockstack-core/sample# clarity-cli check sum.clar /data/db
Checks passed.
root@51db756e5aa7:/src/blockstack-core/sample# clarity-cli launch SP23FEK5XGYT79HKZEDUHF548NYU33FSA3C1QBSM4.sum sum.clar /data/db
Contract initialized!
root@51db756e5aa7:/src/blockstack-core/sample# clarity-cli execute /data/db SP23FEK5XGYT79HKZEDUHF548NYU33FSA3C1QBSM4.sum sum SP23FEK5XGYT79HKZEDUHF548NYU33FSA3C1QBSM4 u108 u18
Transaction executed and committed. Returned: u126
root@51db756e5aa7:/src/blockstack-core/sample#
```

## token.clar代码分析

```

(define-map tokens ((account principal)) ((balance uint)))
;定义对应表
(define-private (get-balance (account principal))
;定义私有方法 获取账户余额
  (default-to u0 (get balance (map-get? tokens (tuple (account account))))))
;设置账户余额为0

(define-private (token-credit! (account principal) (amount uint))
;私有方法 接受转账
  (if (<= amount u0) ;如果小于等于0
    (err "must move positive balance") ;抛出错误
    (let ((current-amount (get-balance account))) ;调用获取账户余额
      (begin
        (map-set tokens (tuple (account account))
          (tuple (balance (+ amount current-amount))))
        (ok amount)))) ;添加账户

(define-public (token-transfer (to principal) (amount uint)) ;转账
  (let ((balance (get-balance tx-sender))) ;查询账户余额
    (if (or (> amount balance) (<= amount u0)) ;检查小于等于0
      (err "must transfer positive balance and possess funds")
      ;抛出错误
      (begin ;执行
        (map-set tokens (tuple (account tx-sender))
          (tuple (balance (- balance amount))))
        (token-credit! to amount))))

(define-public (mint! (amount uint)) ;查询账户
  (let ((balance (get-balance tx-sender))) ;获取余额
    (token-credit! tx-sender amount)) ;接收

(token-credit! 'SZ2J6ZY48GV1EZ5V2V5RB9MP66SW86PYKKQ9H6DPR u10000)
;向SZ2J6ZY48GV1EZ5V2V5RB9MP66SW86PYKKQ9H6DPR转账10000
(token-credit! 'SM2J6ZY48GV1EZ5V2V5RB9MP66SW86PYKKQVX8X0G u300)
;向SM2J6ZY48GV1EZ5V2V5RB9MP66SW86PYKKQVX8X0G转账300

```

## 思考题

- 题目一：根据今天对于智能合约的讲解，你认为智能合约可以解决哪些现有互联网无法解决的问题？又会带来哪些问题？
  - 答：
    - 目前智能合约主要解决互联网公信力的问题，实现代码审计问题。
    - 带新的问题主要有代码更迭是否引起失信问题，代码的安全性的问题。
- 题目二：前六节课的主要内容均为Blockstack V1的架构，本节课为Blockstack V2架构中的一个核心内容，请问你认为V1与V2将如何结合在一起呢？
  - 答：blockstack V1的架构主要解决了用户信息认证与数据存储的，blockstack V2架构主要解决数据运行与计算的问题。V1与V2结合初步完成了虚拟机环境。
- 题目三：如果将本节课的内容应用在过去中心化留言板中，你认为整个留言板的流程图会有什么变化？会增加哪些功能？（建议画出流程图讲解）
  - 答：我认为加入智能合约后，可以增加通过token购买与出手信息的功能（图例下一页）

