

一、简答题

1.

- 1)全称: ACM Transactions on Computer Systems 出版社: ACM
- 2)全称: ACM Transactions on Storage 出版社: ACM
- 3)全称: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems
出版社: IEEE
- 4)全称: IEEE Transactions on Computers 出版社: IEEE
- 5)全称: IEEE Transactions on Parallel and Distributed Systems 出版社: IEEE
- 6)全称: ACM Transactions on Architecture and Code Optimization 出版社: ACM

2.

- 1)发送方先用散列函数生成一个散列值
- 2)发送方用密钥对这个散列值进行加密
- 3)将这个加密之后的散列值作为数字签名和消息一起发送给接收方
- 4)接收方使用和发送方一样的散列函数生成散列值
- 5)接收方用公钥对数字签名进行解密
- 6)接收方比较通过散列函数计算出的散列值和通过公钥对数字签名解密出的散列值

3.

一对一模型可以保证一个线程被阻塞后, 同进程的其他线程仍有可能被调度执行
该模型的优点:

- 1)如果一个线程被阻塞, 内核可以调度同进程中的其他线程执行。
- 2)同进程内的线程并行度好, 可以分别调度到多个处理器上。
- 3)每个线程都有自己独立的资源, 资源利用率高。
- 4)线程之间相互独立, 有助于实现线程安全。

该模型的缺点:

- 1)即使同进程内的线程切换也需要进入核心态执行调度算法。
- 2)当多个线程需要访问共享资源时, 需要使用锁或其他同步机制, 会增大使用的复杂度和计算开销。

二、计算题

1.

(a)

如果A链有n个区块, 则A链的链长为

$$work_A = n \times (2^4 + 2)$$

如果B链有n个区块, 则B链的链长为

$$work_B = n \times 2$$

(b)

区块链网络中的节点会更倾向于选择A链

因为区块链网络会倾向于选择工作量更大的链, 而在同样的区块数的情况下, A链的工作

量大于B链

2.

$a(1,0,0)^T$

$b(2,0,0)^T$

$c(3,1,0)^T$

$d(4,1,0)^T$

$e(5,1,2)^T$

$f(6,1,2)^T$

$g(7,1,2)^T$

$h(0,1,0)^T$

$i(2,2,0)^T$

$j(6,3,2)^T$

$k(0,0,1)^T$

$l(0,0,2)^T$

$m(4,1,3)^T$

三、程序设计题

```
interested[i] = true;
done = false;
passed[i] = false;
loop
    if  $k \neq i$  then
        if not interested[i] then
             $k = i$ 
        end if
    else
        passed[i] = true;
        done = true;
        for  $j = 1 \dots N$  except  $i$  do
            if passed[j] then
                passed[i] = false
                done = false
            end if
        end for
    end if
end loop
CRITICAL SECTION
passed[i] = false;
interested[i] = false;
```

四、实操题

(a)

区块:

#5

随机数:

16979

币基:

¥100.00

->

Sophia

Tx:

¥1

从:

Haoyu Song

->

Yangguang Sh

¥6.00

从:

Ryan

->

Carter

¥4.00

从:

Ryan

->

Riley

¥9.95

从:

Grace

->

Katherine

前指针:

0000c694336f88129f3685bd3ba5d67c445dfd8d18bd22f5d87301dd560e1

哈希:

00007467bd67ecee9c5b37e6fb99d849767e9c3f58b5372f42c8ec4a8b5f1

挖矿

(b)

区块:

#4

随机数:

273125

币基:

¥100.00

->

Anders

Tx:

¥15.00

从:

Jackson

->

Ryan

¥5.00

从:

Emily

->

Madison

¥8.00

从:

Sophia

->

Haoyu Song

前指针:

0000df1d632b734f5a5fc126a0f0e8894fb4c8314ba7086b62980559af67

哈希:

00007c1074a40ce15d89e3d538b4fbb183ae448cf40fe0a3bbff53acc722f

挖矿

区块:

#5

随机数:

30183

币基:

¥100.00

->

Sophia

Tx:

¥1

从:

Haoyu Song

->

Yangguang Sh

¥6.00

从:

Ryan

->

Carter

¥4.00

从:

Ryan

->

Riley

¥9.95

从:

Grace

->

Katherine

前指针:

00007c1074a40ce15d89e3d538b4fbb183ae448cf40fe0a3bbff53acc722f

哈希:

0000913d1a9047529c43e350a67753d93367d3a11eab50568932e819b6e2c

挖矿

(c)

区块:

#4

随机数:

273125

币基:

¥100.00

->

Anders

Tx:

¥15.00

从:

Jackson

->

Ryan

¥5.00

从:

Emily

->

Madison

¥8.00

从:

Sophia

->

Haoyu Song

前指针:

0000df1d632b734f5a5fc126a0f0e8894fb4c8314ba7086b62980559af67

哈希:

00007c1074a40ce15d89e3d538b4fbb183ae448cf40fe0a3bbff53acc722f

挖矿

区块:

#5

随机数:

30183

币基:

¥100.00

->

Sophia

Tx:

¥1

从:

Haoyu Song

->

Yangguang Sh

¥6.00

从:

Ryan

->

Carter

¥4.00

从:

Ryan

->

Riley

¥9.95

从:

Grace

->

Katherine

前指针:

00007c1074a40ce15d89e3d538b4fbb183ae448cf40fe0a3bbff53acc722f

哈希:

0000913d1a9047529c43e350a67753d93367d3a11eab50568932e819b6e2c

挖矿

关于如何高效的验证交易记录的一致性：

- 1) 使用 Merkle Tree
- 2) 让区块链网络中的节点达成共识机制
- 3) 通过散列值和数字签名来验证区块的完整性和真实性