

Smart Contracts

21CSPH0 Blockchain Technology and Applications

Beyond Financial Transactions

- Distributed Ledger Technology (DLTs) can contain information beyond financial transactions
- Submitting executable code as a transaction
- Transaction Execution implies code execution
- Consensus on the code execution

Digital Contracts

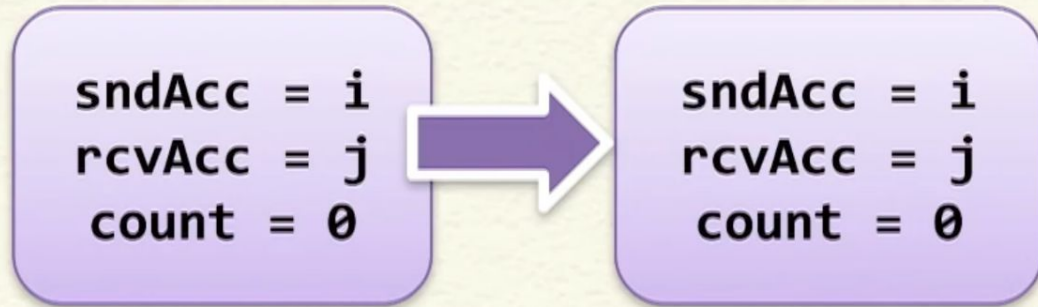
```
int pay (float *sndAcc, float *rcvAcc, float amount) {  
    if (*sndAcc < amount) return -1;  
    else {  
        *sndAcc -= amount;  
        *rcvAcc += amount;  
        return 1;  
    }  
}  
  
int deliverGoods (int count, int pricePerC) {  
    int success = pay (sender, receiver, count*pricePerC);  
    if(success == 1) {  
        scheduleLogistics();  
        return 1;  
    }  
    Return 0;  
}
```

```
int pay (float *sndAcc, float *rcvAcc, float amount) {  
    if (*sndAcc < amount) return -1;  
    else {  
        *sndAcc -= amount;  
        *rcvAcc += amount;  
        return 1;  
    }  
}
```

sndAcc = i
rcvAcc = j
count = 0

```
int deliverGoods (int count, int pricePerC) {  
    int success = pay (sender, receiver, count*pricePerC);  
    if(success == 1) {  
        sceduleLogistics();  
        return 1;  
    }  
    Return 0;  
}
```

```
int pay (float *sndAcc, float *rcvAcc, float amount) {  
    if (*sndAcc < amount) return -1;  
    else {  
        *sndAcc -= amount;  
        *rcvAcc += amount;  
        return 1;  
    }  
}
```



deliverGoods (10, 4)

```
int deliverGoods (int count, int pricePerC) {  
    int success = pay (sender, receiver, count*pricePerC);  
    if(success == 1) {  
        scheduleLogistics();  
        return 1;  
    }  
}
```

State Change with respect to the input

```
int pay (float *sndAcc, float *rcvAcc, float amount) {  
    if (*sndAcc < amount) return -1;  
    else {  
        *sndAcc -= amount;  
        *rcvAcc += amount;  
        return 1;  
    }  
}
```

sndAcc = i
rcvAcc = j
count = 0



sndAcc = i - 40
rcvAcc = j + 40
count = 40

deliverGoods (10, 4)
pay(sndAcc, rcvAcc, 40) > 1

Distributed Code Execution

```
int pay (float *sndAcc, float *rcvAcc, float amount) {  
    if (*sndAcc < amount) return -1;  
    else {  
        *sndAcc -= amount;  
        *rcvAcc += amount;  
        return 1;  
    }  
}
```

```
deliverGoods (10, 4)  
pay(sndAcc, rcvAcc, 40) > 1
```

sndAcc = i
rcvAcc = j
count = 0



sndAcc = i - 40
rcvAcc = j + 40
count = 40

pricePerC {
receive count*pricePerC);

**Put the states of execution
in a blockchain**

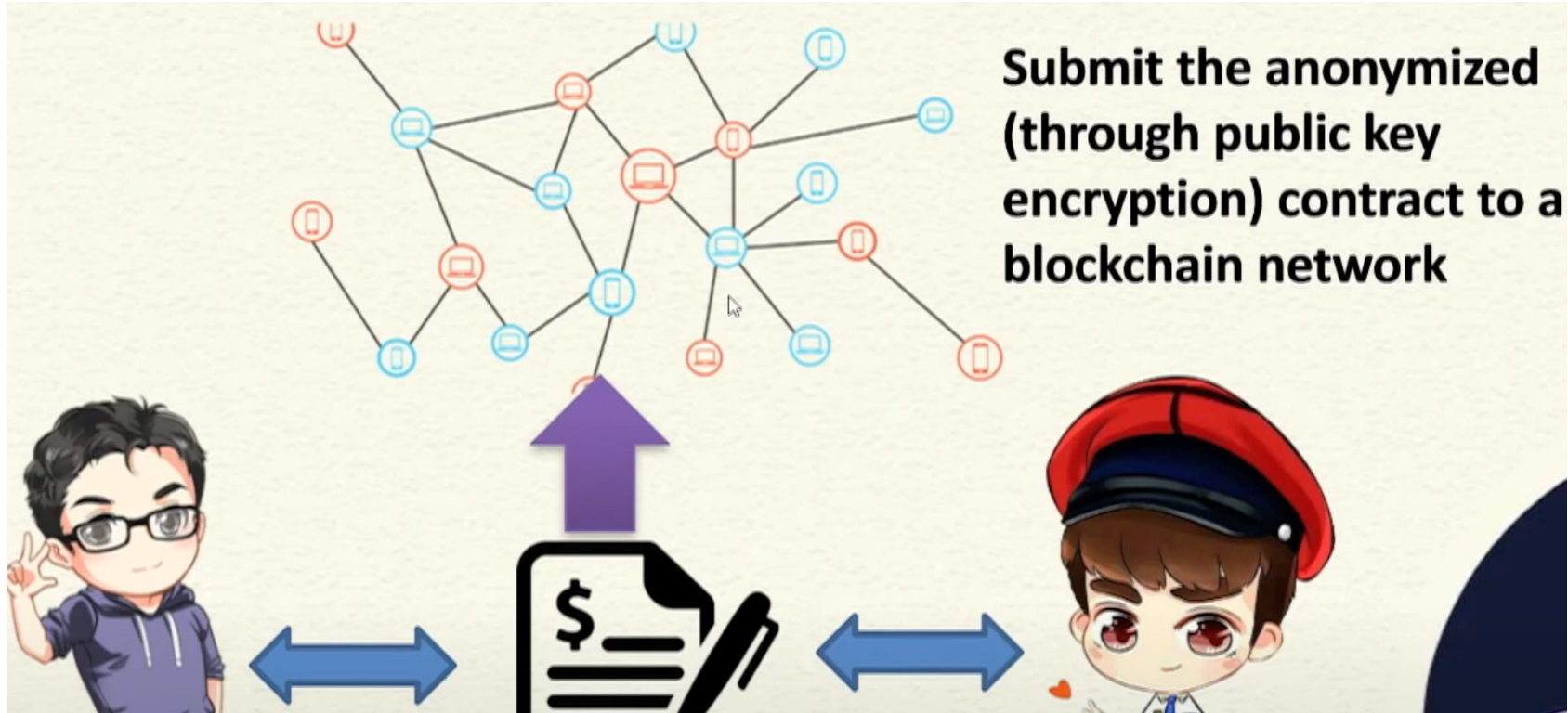
Smart Contracts

Smart Contracts

**Automatically Execute Code over a
Decentralized Platform**



Smart Contract Execution



Smart Contract Execution



**Everyone in the network
can see and validate the
execution steps**

