

# 法律声明

---

- 本课件包括：演示文稿，示例，代码，题库，视频和声音等，小象学院拥有完全知识产权的权利；只限于善意学习者在本课程使用，不得在课程范围外向任何第三方散播。任何其他人或机构不得盗版、复制、仿造其中的创意，我们将保留一切通过法律手段追究违反者的权利。



关注 小象学院

---

# 区块链编程: Solidity以太坊智能合约

王亮

---

# 第四课 solidity编程:智能合约实现

## 4.10 特殊变量和函数

# 地址相关(Address Related)

---

- ❑ `<address>.balance(uint256)`: address 的余额, 以wei为单位。
- ❑ `<address>.transfer(uint256 amount)`: 从合约(地址)向address发送一定数量的ether, 以wei为单位。
- ❑ `<address>.send(uint256 amount) returns (bool)`: 同transfer。不建议。

# 地址相关例子

```
//调用者向合约地址转入 msg.value 个以太币, 单位是 wei  
function deposit() payable returns (address, uint) {  
    return (msg.sender, msg.value);  
}
```

```
//调用者取回value(单位为wei)个以太币  
function draw(uint value) {  
    msg.sender.transfer(value);  
}
```

```
//获得合约的地址和以太币  
function getContractAddrees() constant returns (address, uint) {  
    return (this, this.balance);  
}
```

# 合约相关

---

- ❑ `this`: 当前合约的类型，可以显式的转换为 `Address`。
- ❑ `selfdestruct(address receipt)`: 销毁当前合约，并把它所有资金发送到给定的地址。
- ❑ 如果一个函数需要进行货币操作，必须要带上 `payable` 关键字。

# 数学和加密函数

---

- ❑ `assert(bool condition)`: 如果条件不满足, 抛出异常。
- ❑ `keccak256(...)` returns (bytes32): 使用以太坊的 (Keccak-256) 计算HASH值。常用来做字符串相等判别。

# 特殊变量及函数

---

- ❑ msg.sender (address) 当前调用发起人的地址。
- ❑ msg.value (uint) 这个消息所附带的货币量，单位为wei。
- ❑ tx.origin (address) 交易的发送者。不建议。
- ❑ msg.data (bytes) 完整的调用数据 (calldata)。
- ❑ now (uint) 当前块的时间戳。



# 时间单位

---

- seconds, minutes, hours, days, weeks, years 均可做为后缀，并进行相互转换，默认是seconds为单位。
- 后缀不能用于变量。

# 时间单位

```
function nowInSeconds() returns (uint256) {  
    return now;  
}
```

```
function f(uint start, uint daysAfter) {  
    //时间单位的使用  
    if (now >= start + daysAfter * 1 days) {  
    }  
}
```

# 货币单位

---

- 一个字面量的数字，可以使用后缀wei,finney,szabo或ether来在不同面额中转换。
- 不含任何后缀的默认单位是wei。

# 货币单位

---

- ❑ 1: wei Wei Dai 戴伟 密码学家，发表 B-money
- ❑  $10^3$ : lovelace Ada Lovelace 洛夫莱斯 世界上第一位程序员、诗人拜伦之女
- ❑  $10^6$ : babbage Charles Babbage 巴贝奇 英国数学家、发明家兼机械工程师，提出了差分机与分析机的设计概念，被视为计算机先驱。
- ❑  $10^9$ : shannon Claude Elwood Shannon 香农 美国数学家、电子工程师和密码学家，被誉为信息论的创始人
- ❑  $10^{12}$ : szabo Nick Szabo 尼克萨博 密码学家、智能合约的提出者  
 $10^{15}$ : finney Hal Finney 芬尼 密码学家、工作量证明机制 (POW) 提出
- ❑  $10^{18}$ : ether 以太

# 货币单位

---

```
uint a;
```

```
function f() returns (bool) {  
    if (2 ether == 2000 finney) { //正确  
        return true;  
    }  
  
    return false;  
}
```

---

# 流程演示

# 联系我们

---

## 小象学院：互联网新技术在线教育领航者

— 微信公众号：**小象学院**

