# 分类框架

## 受区块链协议影响

1. 受矿工影响的合约执行结果
2. 交易顺序依赖
3. 重放攻击
4. 私有可见性

## 没有检查的返回值

1. 未处理的异常

## 动态数组操作

1. 删除动态数组元素

## 以太币的单向流动

1. 强制接收以太币
2. 锁定的资金

## 发送以太币时未遵循CEI模式

1. 重入漏洞

## 精度损失

1. 整数除法
2. 整数截断错误

## 缺失或不正确的权限控制

1. 任意写入存储
2. 容易自杀的合约
3. 挥霍的合约（浪子合约）
4. 使用tx.origin进行身份验证

## 被外部控制的调用信息

1. 调用数据被外部控制
2. 调用地址被外部控制
3. 调用数据和调用地址都被外部控制

## 被外部地址Dos

1. 被不存在的地址或死去的合约DOS
2. 复杂的fallback函数

## 不正确的整数运算结果

1. 整数上溢或下溢
2. 整数符号错误

## 使用0.5.0版本以前的编译器带来的问题

1. 在do-while语句使用continue
2. 使用已被废弃的结构
3. 未显式声明的可见性

## 未初始化问题

1. 未初始化的状态变量
2. 本初始化的本地变量
3. 未初始化的存储变量

## 多余的语句

1. 未使用的返回结果
2. 使用uint类型与0比较大小
3. 未使用的变量

## 使用较劣的写法——到此2019-12-15晚

1. 循环不变量
2. Byte[]
3. 未将不变量声明为constant
4. 太多位数字
5. 未将合约内未使用的public函数声明为external
6. 无上限的编译器版本

## 错误的继承

1. 隐藏状态变量
2. 不正确的继承顺序

## 未遵守指定标准

1. View/constant函数改变合约状态（0.5.0版本后会显示编译错误）
2. 不标准的命名规范
3. 不标准的代币标准接口

## 书写错误

1. 拼错构造函数名（0.5.0版本后不允许使用和合约同名的函数充当构造函数）
2. 错误的操作符（+=，和-=，在0.5.0版本之前，错写为=+、=-并不会导致编译错误）

## 使用汇编代码

1. 任意指定函数变量类型
2. 在构造函数中使用汇编代码return(0.5.0版本后会出现编译错误)

## 十九、 被块的gaslimit给Dos

1. 巨大的循环
2. 删除动态数组
3. 不安全的变量类型推断