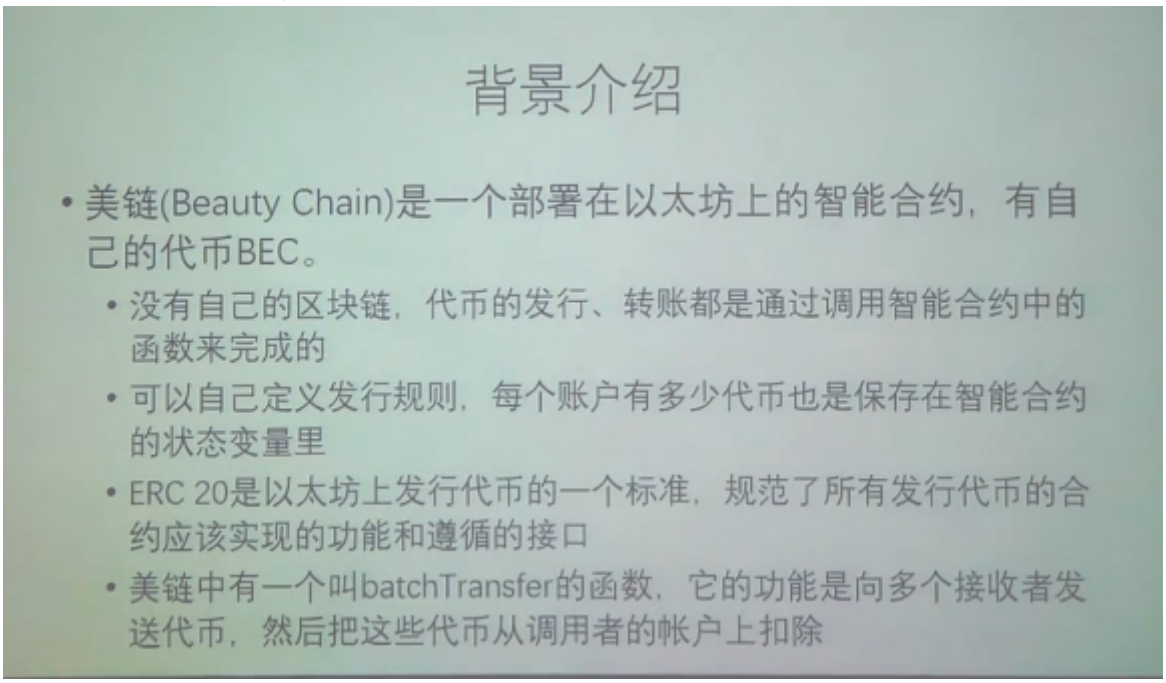
反思

1. smart contract是真的smart吗？其中并不包含AI，准确来说是Auto contract。
2. irrevocable（不可篡改）是一把双刃剑，在中心化领域内，软件升级，发布补丁，银行冻结账户都是可以快速完成的事情，但是在去中心化的情况下，则需要通过软分叉甚至硬分叉来实现。
3. Nothing is irrevocable。在想篡改的区块的前一个区块发起分叉攻击。 比如the DAO事件后的第一种方案，是分叉。
4. solidity语言本身的问题，但现实中自然语言书写的合同也会产生漏洞，所以bug杜绝的途径不应该在语言追求上，而是像合同一样，创建一些针对特定场景的智能合约模板。
5. 透明性（开源）是否真的好？ many eyeball fallacy，很有可能被人误解开源代码一定有很多人看，实际上并不一定如此。
6. what dose decentralized mean？是开发者组织决定还是大多数人投票决定？pow是有挖矿来投票的，但是如果真理在少数人手里，那决定是否公平？
7. 去中心化不等于分布式，去中心化是分布式，但分布式不一定是去中心化。
8. 加密货币不应该和传统支付方式做竞争。而是可是朝着成为一种全球化的货币转换枢纽发展。

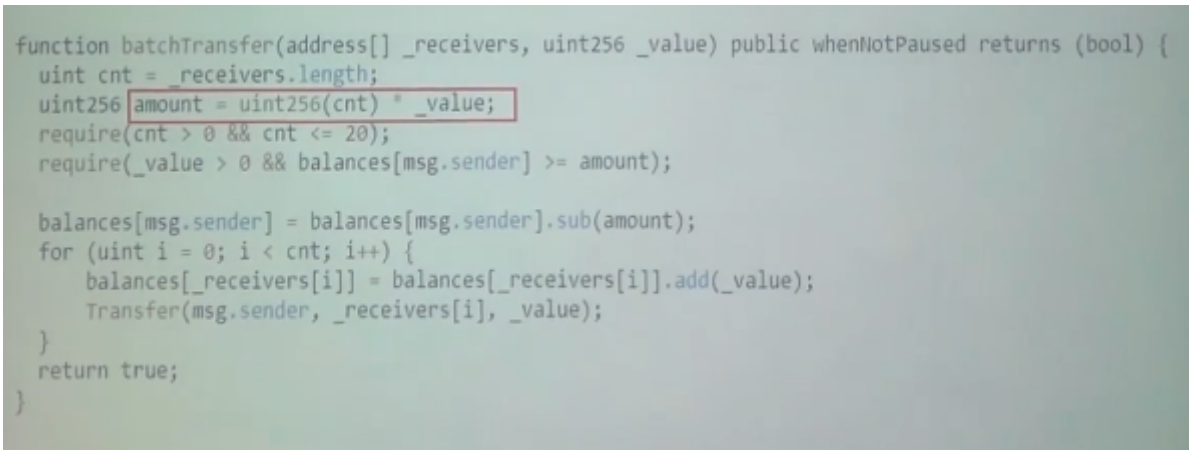
美链——智能h合约的漏洞举例

ICO: initial coin offering



漏洞是代码中代币总数可能溢出，最后可能算出来结果是一个很小得知，但是给各个用户分发时仍然是原来的

值。



```
function batchTransfer(address[] _receivers, uint256 _value) public whenNotPaused returns (bool) {
  uint cnt = _receivers.length;
  uint256 amount = uint256(cnt) * _value;
  require(cnt > 0 && cnt <= 20);
  require(_value > 0 && balances[msg.sender] >= amount);

  balances[msg.sender] = balances[msg.sender].sub(amount);
  for (uint i = 0; i < cnt; i++) {
      balances[_receivers[i]] = balances[_receivers[i]].add(_value);
      Transfer(msg.sender, _receivers[i], _value);
  }
  return true;
}
```