23 ETH The Dao

DAO：Decentralized Autonomous Organization

DAC：Decentralized Autonomous Corporation

The DAO：一个投资众筹组织。可以把以太坊发给The DAO，大家需要投资的时候，集体投票

The DAO一共只存活了三个月。问题出在怎么取回我投资的钱？这个问题在The DAO里面是通过split DAO的方法来实现的。不光是取回投资，而是拆分一个child DAO。这样设计的好处是比如说一小部分人想要投资一个项目（这个项目不被大多数人看好），他们就可以用The DAO的代币去取回他们的以太币，然后用这些以太币去投资新的项目。如果一个个人想取回钱，那么就自己拆分出来一个child DAO，然后把自己取出来的所有以太币投资给自己就可以了。这是The DAO中唯一取回投资的方式，并没有上节课中竞拍合约那种的wtihdraw函数。拆分之前有7天的讨论起，拆分之后有28天的冷静期。

```
function splitDAO(
        uint _proposalID,
        address _newCurator
) noEther onlyTokenholders returns (bool _success) {
        ……
        // Burn DAO Tokens
        Transfer(msg.sender, 0, balances[msg.sender]);
        withdrawRewardFor(msg.sender); // be nice, and get his rewards
        totalSupply -= balances[msg.sender];
        balances[msg.sender] = 0;
        paidOut[msg.sender] = 0;
        return true;
}
```

这个时候就是因为没有提前清零，而是先进行的转账，导致黑客可以进行重入攻击。正是因为这样的写法，导致The DAO在众筹到价值1.5亿美金的以太坊之后，被黑客攻击转走了大概价值5000万美金的以太坊。对于这样的做法，以太坊社区内分为两派来讨论如何解决这个问题，一部分人认为应该回滚这个交易，来保证大部分人的利益，另一部分人认为黑客的行为并没有违法（因为code is law），只是利用了代码当中的特性，所以不应该采取任何的措施。

以太坊的开发团队Vitalik他们，是支持回滚的。因为The DAO占用的比特币总数量大概百分之十几，所以不希望黑客持有这么大的以太坊。Too big to fail，如果The DAO垮了，会对以太坊社区造成很大的影响，所以必须补救。（类似于国家不会让大企业倒闭一样）。

但我们应该从哪个区块开始回滚呢？不能直接从黑客发起攻击前的区块直接分叉，因为会导致一些其他的交易也被回滚，这样的话就乱套了。所以必须精确定位那些黑客的交易，只回滚那些。怎么做呢？需要分为两步，第一步需要锁定黑客的账户，第二步就是把黑客得到的钱退回去。

为了实现第一步，以太坊系统发布了新的升级，所有和The DAO有关联的账户都不能进行交易。这属于软分叉还是硬分叉？这个是软分叉，因为旧版本的节点依然会接受新版本节点发布的交易。这个想法很好，但是有个bug。就是升级后的节点判断一个交易是和The DAO相关的话，如果交易是非法的，还要不要收取gas fee？正常情况下，gas fee的设置是为了防止denial service attack，防止大量了非法交易进行冲击而浪费矿工的资源。而实际上升级之后判断The DAO相关的账户为非法交易是并没有收取汽油费。导致网上出现了大量的这种denial service attack。导致大量矿工降级版本，导致这个软分叉的版本失败了。

设计了新的硬分叉的版本，就是强制把The DAO上面的所有钱都转到一个新的智能合约上面，而这个智能合约唯一的作用就是退钱。在升级的软件当中，写死一条规则就是挖到第192万个区块的时候，把The DAO上面的钱转到这个新的智能合约上面（因为是写死在升级里面，所以不需要签名之类的了，有点儿类似于法院的强制执行）。这个时候没有升级的矿工就不会认可新的区块，因为没有合法的签名，所以是非法的交易。

这个引起了非常激烈的讨论，因为这和中心化的做法没有区别。所以最后以太坊的开发团队通过智能合约来进行投票，结果是大部分的矿工还是支持硬分叉的，并且升级了软件。最后挖到第192万个区块的时候实现了硬分叉，这样最终黑客的攻击是没有成功的。

但这个故事并没有结束，少数不支持硬分叉的人还留在旧链上面挖，然后一部分交易所开始上市这个旧链上面挖出来的币。旧链上面的币称为ETC，Ethereum classic，一部分是为了投机，但还有一部分人是为了信仰，就是坚信完全的去中心化。新链上面的币还是继承了原来的叫法，称为ETH。

一开始的时候出现了很大的问题，因为旧链和新链用的是同一套系统，同一套公私钥对的体系，所以旧链上面的交易也可以拿到新链上面做重放攻击，新链上面的交易也可以拿到旧链上面进行重放攻击，导致了很大的混乱。所以就给每个链都加了chain ID，就变成了完全的两条链。

之所以需要将The DAO中的所有账户的钱都转到新的合约上面，是因为如果只转黑客的，而其他的账户还在运转的话，那么任何一个账户都有可能称为新的黑客。而全部转走的目的就在于作废The DAO的合约（因为合约代码不能篡改，只能直接不用了）。