比特币实现了[去中心化](https://so.csdn.net/so/search?q=%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96&spm=1001.2101.3001.7020" \t "_blank)的货币，以太坊实现了区中心化的合约，产生了一个新概念，let's dencentralized enerything. DAO概念就是在这个背景中产生的。

1. **DAO——dencentralized Autonomous Organization**

传统社会当中组织是建立在某种法律文件基础上，区块链上DAO去中心化自制组织就是建立在代码基础上的，组织的规章制度是写在代码里的，通过区块链的共识协议来维护规章制度的正常执行。

1. **The DAO: 2016年的众筹投资的组织**

The DAO有点像众筹的投资基金，只不过投资的钱的来源是在区块链上大家众筹的方法得到的，本质是运行在以太坊的智能合约。如果想参与The DAO，可以把以太币发给智能合约，换会The DAO的代币，需要决定投资的项目是大家投票决定的，代币越多投票的权重越大，投资有了收益也是按照智能合约当中规定的分配制度分配利润。

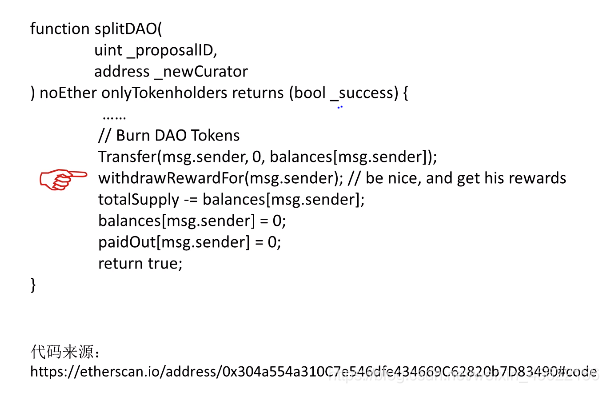
DAC：Dencentralized Autonomous Corporation，和DAO类似，但是DAC是出于盈利目的的，DAO的话可以是出于非盈利目的，比如公益事业。DAC在现实中并不具有公司具有的法人地位。

The DAO设立初期的筹集速度非常快，比传统的众筹网站快很多。但是The DAO只存活了三个月，问题出现在哪里？

比如说你是一个The DAO的投资者，如何取回之前的投资和收益？The DAO基金里采用拆分的方法实现，split the DAO，也是一种建立子基金的方法，叫child DAO。设计理念是这样的，The DAO的投资项目是大家用手里的代币投票决定的，如果有一小部分人的投资理念和大家不一样，这一小部分就可以用拆分的方法从The DAO里面独立出来，成立一个自己的子基金，叫child DAO，拆分的时候他们手中的代币是要被收回去的，然后换成相应数量的以太币，然后用这些以太币成立子基金，就可以投自己想投的项目了。拆分的极端案例就是一个人单个成立一个子基金，也就是child DAO只有他一个人，这也是投资者取回投资和收益的唯一途径，The DAO没有设置withdraw函数，所以只能用拆分的方法取回投资。拆分之前有7天的辩论期，讨论拆分的合理性，可加入性等；拆分之后有28天的锁定期，28天之后以太币才能被取出来。

**拆分的理念是没有问题的，问题出现在了split DAO的代码实现上。**

1. **Split DAO代码存在的漏洞**



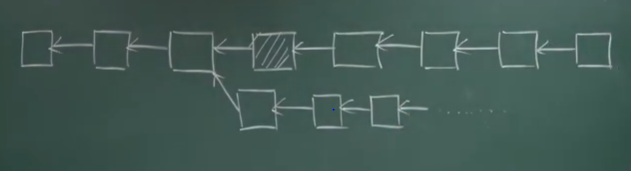
withdraw是先把钱还给调用这个函数的人，然后把The DAO中的总金额减少相应的数量，再把调用的账户清0。应该做的是先把账户清0，然后再转账，黑客就是利用这个漏洞进行了重入攻击，转走了五千万以太币。

1. **以太坊对The DAO事件的应对**

事件发生之后就开始讨论是否要利用这28天的时间回滚交易，一方认为回滚，另一方认为不用，因为只是以太坊的一个智能合约出现了漏洞，坚持维护不可篡改。Vitalik Buterin团队认为因为该事件影响非常大，The DAO又占据了超过10%的以太币，too big to fail，所以还是决定回滚了交易。

**问题是如何补救呢？**

分叉攻击，在被黑客攻击前的一个区块开始挖，直到长于原来的那条链。但是这样是不可行的，因为原来的那条链上还是有很多其他合法的交易，一旦回滚就导致全部交易都回滚，不仅仅是黑客攻击的交易。



补救原则：回滚必须精确定位，只能是回滚黑客盗取以太币的交易，其他发生的正常交易不能受到影响。

第一步：锁定黑客的账户

第二步：把黑客盗走的以太币撤回去，清退The DAO基金的钱。

以太坊团队发布了一个软件升级，在这个升级的软件里增加了一条规则，凡是跟The DAO这个基金账户相关的，不允许做任何交易。这是一个**软分叉(旧矿工认可即为软分叉)**，因为是加了一条交易规则，更新的矿工挖出的区块旧矿工是认可的，因为旧矿工不知道这个规则，但是旧矿工挖出的区块新矿工有可能不认可。遗憾的是这个升级的系统有一个bug，是关于和The DAO相关的交易要不要收取汽油费的问题，在本次升级中以太坊团队没有设置收取汽油费，这导致整个以太坊受到了大量的denial of service攻击，许多矿工便选择回滚到软件升级前的版本，从而导致软分叉失败。

软分叉方案失败之后，以太坊团队决定采取硬分叉，把整个以太坊区块链分裂成两条。通过软件升级把The DAO账户上的所有资金强行转到另外一个新的智能合约上去，新的智能合约只有一个功能就是退钱，把代币退回成以太币。用软件升级的方法强行重新记账，本来转账要有合法的签名，这里就不管这些了，凡是The DAO账户的资金，不管本人同意不同意都要强行转到新的智能合约上去，升级的软件规定了强制执行的具体的日期，挖到第192w块个区块的时候，自动执行不需要合法签名。由于这次升级旧矿工是不认可这些区块中交易的，因此属于硬分叉。

最后整个以太坊分成了两派，分为支持硬分叉和不支持硬分叉的两队，在经过整个社区的投票之后决定进行硬分叉。

1. **ETH and ETC(ehtereum classic)**

但是还是有一部分人决定维护”真正的“以太坊，所以导致以太坊现在是新旧链并存。这样就导致分叉初期出现很多重放攻击，因为两条链的代码账本和私钥都是一样的。后来给两条链上加了chain id，从此分成了两条完全独立的区块链。

Question: 不论是硬分叉还是软分叉，为什么不单单冻结黑客账户，要冻结The DAO智能合约的全部账户和交易？

Answer: 因为The DAO这个智能合约是有bug的，而且这个bug是没有办法修复的(区块链不可篡改，必须要让整个合约都作废才可以)。为了防止DAO中其他用户模仿黑客的手段进行盗币，以太坊开发团队决定冻结所有The DAO相关的账户和交易。