24 ETH 反思

智能合约其实没有用到任何的AI技术，只是一种自动执行的代码。而且挺笨的，因为没办法修改。

Is smart contract really smart?
Smart contract is anything but smart.

Irrevocability is a double edged sword. 软件的升级需要硬分叉，而不像中心化系统那么方便。硬分叉需要说明理由，很有可能泄露安全隐患所在。还有可能没来得及修好就被攻击了。

像The DAO这种，就是黑客只偷走了1/3，还有2/3在The DAO的合约上面，就有人建议一个好人用黑客同样的方法把剩下的钱转到一个安全的合约上面。

Nothing is irrevocable。比如说分叉攻击。这一次The DAO是以太坊的开发团队通过软件升级的硬分叉方式，强行的改变某些用户的状态。所以没有什么是改不了的。一般不会改，但是必要的时候还是得改的。

语言设计上有什么需要改进的？solidity语言是反自然的，我给你转账实际上是调用了你的fallback函数，导致你还可以反过来调用我。正常来说我给你转账只需要调用自己的函数就可以了。

solidity语言设计上有什么问题？Is solidity the right programming lanaugage? 比如说Ocaml，functional programming的语言。用formal verification来证明一个代码只能干指定的事情。

Turing completable是不是必要的？选一个适中的，不能太简单，还能实现智能合约的所有应用场景。还有就是比如说现实生活中写合同也没有专门的语言，而是有一些模板。未来可能会出现类似于律师事务所这种的，专门来帮助你写合同的。

去中心化的系统是透明的，开源的，而中心化往往是不开源的。开源的好处就是增加公信力，接受大家的监督。开源的代码不容易出现漏洞，有很多人监督。但其实很多开源软件都有很多安全漏洞。Many eyeball fallacy。其实真正会看源代码的人非常少，而且可能看代码的人的专业知识不够，所以看不出来漏洞。开源软件不一定比不开源软件安全。很多人用的软件也不一定是安全的。

区块链的追随者很多都是去中心化管理的拥护者。What does decentralization mean? 像The DAO的修改能成功的原因并不是因为以太坊的开发团队强制大家接受， 而是大部分人都同意了。所以去中心化并不是让代码来减少人为的干预，而是需要通过去中心化的机制来让大家来同意修改。

其实分叉也是去中心化的一种表现。因为只要你自己不同意，你就可以分叉。这样的话即便是少数人的利益也可以得到保障，恰恰是民主的一种体现。

decentralized 不等于distributed。一个去中心化的系统一定是分布式的，但是一个分布式的系统不一定是去中心化的。因为可能一个分布式的系统所有server都是有一个机构来持有的。

状态机最早的应用场景是mission critical applications，比如说airtraffic control, stock exchange, space shuttle。必须无间断的对外提供操作，这个时候就需要很多状态机一起工作，即使一台down了，其他的也可以工作。而且几组状态机一起工作的效率比一台计算机的效率低，因为需要同步状态。但是这样可以保证整个系统无间断的对外提供服务。