北京大学肖臻老师《区块链技术与应用》公开课笔记

> 反思，对应肖老师视频：click here
> 全系列笔记请见：click here
> **About Me:**点击进入我的Personal Page

关于智能合约的反思

Is smart contract really smart?

智能合约与人工智能无关，其本质上是"自动合约"——以事先写好代码自动执行相应规则。因此，智能合约并不智能，写好之后就不可以再进行修改，实际上就相当于一个"代码合同"。

反思一：smart contract is anything but smart

正是区块链的不可篡改性，导致对笔记28中提到The DAO中的bug也无法进行修改，最终酿就以太坊的硬分叉。

设想你发现银行卡信息被盗，第一反应是通知银行将账户进行冻结。但如果在区块链上，你就只能眼睁睁看着账户中的钱被转移走。

> 当时1/3的钱被黑客转走后，除了联系以太坊团队还能怎么补救？
>
> 由于无法阻止其他人继续调用智能合约，因此必须将智能合约中的钱转走。而智能合约并没有提供转走钱的方法，那就只能通过黑客的方法将剩余资金转移到新账户中。

反思二：Irrevocability is a double edged sword

我们说不可篡改性是双刃剑，但真的有什么是不可篡改的吗？分叉攻击不就是一种篡改方式吗？以太坊团队通过软件升级强行修改账户状态，实现在未经他人许可下转走别人的钱。

因此，不要迷信区块链的不可篡改性，毕竟，代码是死的，而人是活的。没有什么无法被修改，即使是一个国家的根本大法——宪法都可以被修宪。如美国曾经有个第18修正案实施禁酒令，然而十几年后在第24修正案中就被推翻了。

一般来说，区块链上内容难以篡改，但真正遇到类似The DAO这类重大事件，真正想要修改还是可以实现的。

反思三：Nothing is irrevocability

关于语言设计的反思

为什么会出现"重入攻击"？某种意义上来说，solidity语言的特性是反人类直觉的。一般意义上，A给B转账，B不可能会反过来调用A。然而solidity语言中，A给B转账等于隐性调用了B的failback()函数，而B可以通过fallback()来反过来调用A。由于这与人类常识不符，便容易忽视掉这一漏洞。

有人提出，应该使用函数式的编程语言，因为函数式语言较为安全，不容易出现类似的安全漏洞，且长远来看，要实现对智能合约理论上正确性的证明。

然而，虽然solidity设计存在缺陷，但是否需要采用函数式编程仍然有待探讨。

反思四：Is solidity the right programming language?

比特币脚本语言简单、表达能力差，很多功能无法表达出现。而以太坊的编程语言是图灵完备的，凡是计算机程序可以完成的，solidity都可以将其实现。然而，图灵完备的表达能力是一种好事吗？

有人认为应该选择一种适中的语言，既不要比特币脚本语言那么简单，又不要solidity语言那样图灵完备，希望既可以实现智能合约想要实现的功能，但又不容易出现安全漏洞。然而，找到这样一种语言是困难的，因为设计之初我们无法预料到未来的所有应用场景和所有的安全攻击。

现实生活中是如何解决的？合同语言不够严谨导致执行出现纠纷，我们并未提供一种专门用于合同编写的专用语言，而是通过提供【模板】来解决。

这可能是智能合约未来的发展方向，常用的智能合约可能会出现模板，也可能会出现专门编写智能合约的机构。

反思五：智能合约的历史较短，未来会逐步走向成熟。

关于开源的反思

中心化系统经常是非开源的，好比BAT不会公开他们的软件架构一样。而去中心化需要其他人都执行一致的操作，就必然要开源自己的代码，否则不会被大家所信任。

有人认为，开源还有一个好处——安全。因为开源代码被众人所审视，其中出现安全漏洞的可能不大。

然而，我们已经观察到智能合约代码出现漏洞，其他领域诸多开源软件也出现了各种问题，这就引发我们思考：为什么全世界这么多人在看着这些代码，他们还是出现了这么多漏洞呢？（many eyeball fallacy）

理论上大家都可以去看，然而实际上真正有时间和精力查看的人很少，即使看，也不一定大多数人都又足够的专业知识看出其中隐藏的漏洞。有可能我们都认为世界上这么多人，别人肯定看过了，但实际上大家可能都这么想，没有几个人真正看过开源代码。所以：

反思六：不要认为开源软件必然比非开源软件安全。

关于去中心化的反思

追随区块链技术者，一般也都是去中心化理念的拥护者。这些人对于现实中中心化的弊端有所认识，便追随去中心化这一全新管理模式。这也就是为什么在以太坊推出硬分叉后引发巨大分歧的原因，因为仅凭开发团队通过一个软件升级就可以将别人账上钱强行转走了，这就回到了中心化的老路之上，甚至更加中心化，因为现实中要没收他人财产还需要经过司法程序，28天未必能完成。

但思考一下，硬分叉是单单依靠以太坊开发团队就可以完成吗？What does decentrtilization mean? 以太坊团队发布升级为什么最终能够成功？因为绝大多数矿工接受了升级软件，以行动支持了分叉方案。即使如此，以太坊团队仍然不能阻止另外一部分人从旧链转移到新链上来。

因此，去中心化不意味着完全拒绝人的干预，不意味着完全不能修改，而是要用去中心化的方法来完成修改。

关于分叉的反思

一般认为，分叉是一件坏事，分叉导致原有一条链变成了两条。然而，分叉恰恰是去中心化的体现，在中心化系统中，用户是无法进行分叉的，只能选择放弃和接受。

> 关于以太坊为什么被V神创建的故事：
>
> 19岁时，喜爱玩魔兽游戏，然而魔兽世界将术士一个技能改掉了。他多次联系暴雪公司反馈，然而暴雪对此并未进行答复。因此，他放弃游戏并反思中心化的缺点，并决定创建去中心化平台，用户不满意就可以进行分叉。

因此，存在分叉，恰恰是民主精神的体现。

关于去中心化和分布式

decentralized ≠ detributed

一个去中心化系统必然是分布式的，但分布式未必是去中心化。例如百度、阿里、google等都有着大量的分布式应用，依托于成千数万的服务器运行，但这些都掌握在公司自己手中，这仍然是中心化的。

比特币、以太坊都属于交易驱动的状态机。特点是使得系统中大量节点，通过付出大量代价共同维护相同的状态；然而常用的分布式是多台机器完成不同的工作，从而联合起来完成一个大的任务，从而实现大于单台机器的运算能力。

而状态机是维护所有节点共同状态，多台机器完成同一组操作，即使其中一台机器宕机其余机器仍然可以对外提供完整服务，从而满足一些必须24小时对外提供服务的要求。代价是多态计算机合起来，效率反而小于一台计算机。因此，传统应用状态机场景，机器数量较少，从而减少状态对齐付出的代价。而比特币、以太坊这种控制大规模机器是前所未有的。

基于此，可见比特币、以太坊并不适用于大规模计算和大规模存储。智能合约是编写控制逻辑的，只有在互不信任的单位之间需要建立共识的操作才需要写在智能合约中。