第18讲 | 智能合约与以太坊

2018-05-04 陈浩

深入浅出区块链

进入课程 >

讲述：黄洲君

时长 12:02　大小 4.14M

在前面的文章里，我们介绍了区块链的核心技术，也穿插介绍了一些项目。然而每个区块链都有自己的特色，接下来我们将针对每个项目进行详细讲解。今天我们就来讲讲智能合约和以太坊项目。

今天我们从智能合约这个概念入手，聊聊什么是以太坊项目以及它的发展历史。最后还会介绍几款钱包给你，希望通过今天文章的讲解，你也可以尝试在以太坊上编写简单的智能合约。

智能合约的概念

不同于法律意义上的合约概念，区块链领域的合约表达的是可以“自治自理”的 计算机协议，这套协议具有自我执行、自我验证的属性。

如果完全从技术角度来看，智能合约等价于一段事先就被规定好逻辑和条款的计算机代码被激活运行的状态，同时，智能合约也提供了通用的用户接口，用户可以通过接口与用户交互。

智能合约这一概念早在 20 世纪 90 年代就有人提出，这个人是从事智能合约和数字货币研究的尼克萨博（Nick Szabo）博士，尼克 1996 年在《Extopy》期刊上发表了对智能合约的描述，他认为智能合约是一个由数字表单指定的承诺，这个承诺包含关系到多方执行的一组协议。

从定义中我们可以得知，智能合约由多个协议组成，这些协议包含了用户接口，能表达用户的承诺，它可以安全有效地确定公共网络上的关系。

换句话说，智能合约是一个由计算机处理、可执行合约条款的交易协议，其总体目标是□满足协议既定的条件，例如支付、抵押、保密协议。这可以降低合约欺诈造成的损失，降低仲裁和强制执行所产生的成本以及其他的交易成本。

我们举个实际的例子解释一下，今年 4 月 9 日，上海某建设银行支行开放了“无人□银行”，银行中充斥了众多机器和显示屏，智慧柜员机、VTM 机、外汇兑换机、VR 设备和两台机器人代替了传统的柜台。

这里的智慧柜员机、外汇兑换机器人众多电子设备都可以认为是智能合约的一种表现形式，用户在办理银行业务时，如办理大额汇兑业务，业务流程和逻辑依据已经定在程序中，用户只需要按照操作一步一步进行，办理完成后即可获得单据。

这里“既定的业务流程、机器人模样的人机交互界面、双方同意承诺”组成了智能合约的概念，它甚至具有一定的法律效力。

萨博提出的是智能合约的概念，以及我们举的例子，都是广义的智能合约概念。智能合约具有多种实践形式，而在区块领域所说的智能合约概念，我们其实是指 Blockchain-based 这种形式。

在萨博的智能合约概念中提到了开放式网络，而我们知道开放式网络的基本要求就是拜占庭容错，通过前面文章的讲解我们知道，区块链天然具有拜占庭容错特性。所以如果在区块链上实践智能合约这个概念，两者会非常契合，天造地设。

首先实践了智能合约这一概念的是比特币，比特币脚本（bitcoin script）包含了 5 种标准交易脚本，这些脚本的功能不仅仅提供了普通单人支付的情况，它还提供了多方共同签名支付的脚本，叫做多重签名支付，多重签名支付可以看成是萨博语义下的智能合约。

除了比特币，发扬光大智能合约这个概念的区块链项目就是以太坊了，下面，我重点来介绍一下以太坊项目。

以太坊及其发展历史

以太坊 Ethereum 项目的目标是打造一个去中心化的新一代互联网应用平台，这个平台称作 Dapp 平台。

这些 Dapp 基于以太坊智能合约虚拟机开发、编译、部署，并且可以自定义业务逻辑，部署后全网可见且自动执行，理想情况下不存在宕机、审查、欺诈、第三方干预的情况。

2013 年底以太坊的创始人 Vitalik 在比特币开发者社区提出了可以运行图灵完备（Turing-complete）形式的应用，但这一思想并没有得到比特币社区的支持。

2014 年，Vitalik 带着自己的想法，宣布以太坊项目正式成立，2014 年上半年开始筹集资金，聚拢一些早期开发者，同年 7 月份□进行了为期 42 天的 ICO，共筹集了超过 1800 万美元的比特币。

2015 年 7 月，第一个版本的以太坊发布，主网正式上线，这一阶段 Bug 和设计缺陷较多，多是开发者在使用。

2016 年以太坊发布第二个大版本 Homestead，用户逐渐多了起来，同期也吸纳了不少 Dapp 开发者。

2016 年 6 月，以太坊上发生了著名的黑天鹅事件——TheDAO 事件，这打开了 ICO 市场，同时也造成了以太坊社区分叉，形成了以太坊和以太坊经典两个代币。

2017 年 4 月，ICO 风靡中国，ERC20 提供了低成本方便高效的资金募集方式，为 ICO 提供了极大的便利，趁着数字货币牛市，以太坊的价格涨幅达十多倍，2018 年 1 月以太坊价格突破 1000 美元。

以太坊的核心概念

以太坊核心概念包括：智能合约虚拟机 EVM 和 Solidity 编程语言、账户模型、以太币和 Gas，交易和消息。

1. 智能合约虚拟机 EVM 和 Solidity 编程语言

以太坊的核心概念首先是智能合约。

智能合约包含两部分，一部分是开发语言，主要以 Solidity 为主，Solidity 与 Javascript 语言在使用上十分接近，这极大地降低了 Dapp 开发人员的学习成本。

Dapp 开发者编写好代码以后，使用 Solidity 编译成十六进制字节码，然后部署到 EVM 上，也就是把合约广播到全网，等矿工打包后就形成了常年运行的 Dapp 了。

另一部分就是 EVM。 EVM 是以太坊智能合约虚拟机，我们可以等价理解它为 Javascript、Python 等脚本语言的执行引擎。

它是一个轻量级的虚拟机隔离环境，它并不提供访问本地网络、进程、文件系统的功能，它更像是一个封闭的容器，这个容器里面装了一个正在运行 Dapp，可以□看成是无法和外界交互的 Docker Container。

Dapp 在运行过程中，可以被请求或其他事件触发，然后□执行相应的逻辑，这些请求和事件是由以太坊上的交易产生的，不是来自本地操作系统的事件。

Dapp 运行过程中，每次状态发生变化，则意味着全网同步更新，大家的计算结果都是一致的，这有两个特性：

1. 所有 Dapp 的计算结果经过全网共识，一旦确认过几乎无法被伪造和篡改；
2. 由于必须经过全网共识，所以这限制了整个网络的容量。

2. 账户模型

以太坊并没有采用 UTXO 模型，也不同于银行账户，它是由以太坊开发者设计了自己的账户模型。

以太坊上的账户有两种类型，第一类叫做合约账户 CA（Contracts Accounts)，第二类叫做外部账户 EOA（Externally Owned Accounts）。

简单理解就是□：CA 是智能合约代码用的账户，EOA 是人用的账户；所以 CA 可以存储并执行智能合约代码，它的智能被 EOA 激活，它也不保存和存储私钥，合约账户可以调用其

他合约。

EOA 则是人们直接控制的账户，可以存储以太币，可以发送交易到合约账户，触发既定的逻辑。EOA 账户由公钥标识，由对应的私钥控制。

当合约账户被调用时，存储其中的智能合约可以在矿工处的虚拟机中自动执行，并消耗 Gas，如果 Gas 不足则会触发“Out of Gas”异常，被终止执行。

无论是 CA 还是 EOA，在以太坊内部都被看做状态对象（state objects），意思就是说这些账户都有自己的状态，EOA 具有以太币余额的状态，而 CA 除了余额，还多了合约存储状态。

3. 以太币和 Gas

Gas 是执行智能合约操作的燃料，□智能合约的每一个步骤都会消耗 Gas，Gas 是由以太坊的平台代币以太币转化□而来，最小单位是 wei，1ETH 相当于 10 的 18 次方 wei。

以太币可以通过 PoW 挖矿而产生，目前以太坊主要通过 GPU 挖矿。挖出一个块可以换得 5 个以太币，并且还有一定的交易费、以及叔伯块的奖励。今年 4 月 6 日爆出著名矿机芯片厂商比特大陆已经开发出针对以太坊的 ASIC 专业矿机，相比 GPU 的效率提升 2.5 倍。

4. 交易和消息

以太坊上的交易与比特币中的 UTXO 交易不同，它是指 EOA 账户将一个经过签名的数据包发送到另外一个账户的过程，这个过程产生的账户状态变化将被存储到以太坊区块链上。

以太坊上除了交易还有消息这个概念，消息指一个合约账户调用其他合约账户的过程，可以类比函数调用过程。

所以以太坊上的 Dapp 如果被触发，有两种可能，第一种是交易触发，第二种是消息触发。

这两种的区别在于前者是 EOA 发起的，后者只能是其他合约账户发起的。

状态对象的状态变化被以太坊共识机制的记录下来，交易和消息驱动着状态的变化，于是，□在一个开放式的网络中构建一个全球共享的 Dapp 变得十分方便。

以太坊上智能合约□具有全网准实时同步、准确执行、去中心化运行、较低的人为干预风险等特性，EVM 和 Solidity 为□全球开发者提供了较低的进入门槛。

与比特币的主要区别

以太坊项目又被称作区块链 2.0 项目，这里 2.0 就是指智能合约。那么以太坊与比特币相比，到底智能在那里呢？我们具体来看看。

与比特币相比，以太坊首先不是一个单纯的数字货币项目，它可以提供全世界无差别的区块链智能合约应用平台，这个平台基于我们前面文章所介绍的区块链四大核心技术要素，即 P2P 网络、共识机制、账户模型、加密模块。

除了以上的四个技术要素，以太坊还推出了 EVM——以太坊智能合约虚拟机，并且，它还推出了自己的智能合约语言 Solidity。

于是，区块链的开发者因为智能合约的出现开始分为两类。第一类是公链底层开发者，主要是以 C++ 和 Go 语言为主的全节点开发者，他们需要对区块链各个技术模块有很深的理解。

第二类是智能合约开发者，也就是应用开发者，这类开发者对区块链的运行原理不需要理解很深，只需要会编写 Solidity，了解规范即可。

除了以太坊智能合约这个概念以外，它还设计了下面的内容。

1. 研究并实现了自己的 PoW 挖矿算法——ETHASH，这是一个内存困难型的挖矿算法。
2. 叔伯块激励机制，降低了挖矿中心化的趋势。 取消了 UTXO 模型，采用了账户模型和世界状态，提供了数据结构的可塑性。
3. 设计了 Gas 机制，避免程序死循环消耗全网资源的情况出现。 研究并实现了自己的 PoS 共识算法——Casper，可防止 Nothing-at-Stake 攻击。
4. 以太坊提供了在区块链自由编程的能力，智能合约让所有人得以开发属于自己的 Dapp，这是与比特币作为单纯的数字货币所不具有的能力。

总结

本篇我们介绍了智能合约的概念以及以太坊项目，并且讲解了与比特币的主要区别，以太坊上的一些核心概念，下一篇我们将结合实际案例讲解智能合约，带领你认识一些智能合约模

板，并顺便介绍一下其他区块链智能合约平台。

亲爱的读者，快来构想一下属于自己的智能合约 Dapp 吧。你可以给我留言，我们一起讨论。

参考链接：

https://en.wikipedia.org/wiki/Smart_contract
http://tech.ifeng.com/a/20180413/44947993_0.shtml

上一篇 第17讲 | 去中心化与区块链交易性能

下一篇 第19讲 | 上手搭建一条自己的智能合约

精选留言 (9)

写留言

阿痕
2018-05-10

5

在第15讲《PoW》中提到以太坊采用的ETHASH算法是内存困难型算法，可以有效遏制专业矿机的出现。而本文又说以太坊当前主要基于GPU挖矿，甚至还出现了ASIC的专业芯片，是否有矛盾呢?

展开

作者回复: 不冲突，ethash的结果是出现了只有2.5倍的asic，正常的asic在千倍以上。遏制但是不能避免。

_LeoHuang
2018-05-09

3

https://www.jianshu.com/p/51bc09cb663a 嗯，学习还是需要动手实践，这个是我学习的记录，希望对一起学习的朋友有所帮助

万总
2018-08-16

请问叔伯块（uncles）奖励机制为什么能起到制约中心化挖矿的作用？我记得以太坊区块链一个区块好像只能关联2个叔伯块。

作者回复: 因为可以让矿池更分散，不至于过度集中。从排除的角度考虑，即使没有出块的矿池，也排除了错误的答案，仍旧奖励的话就会鼓励矿池更算力分散而不是集中。

尼古拉斯•...
2018-07-06

老师好！我最近在搭建以太坊在ubuntu16.04上的开发环境，现在是想用源码的方式安装个cpp-ethereum客户端。经过下载代码、安装依赖、编译这几个步骤后，总要不到生成的eth可执行文件。所以请问老师，有没有更好的资料推荐一下～让我把以太坊的C++开发环境搭建起来?

另外一个问题，我想问一下，以太坊钱包Mist、以太坊应用浏览器、以太坊客户端这...

展开

阿痕
2018-05-14

矿工执行智能合约，为什么不直接消耗以太币，而是Gas，Gas机制的目的是什么?

作者回复: 为了平衡合约执行的

无念
2018-05-10

如果有bug的合约程序发布到区块链中，是不是会产生持续性的不良影响

展开

作者回复: 是的，只能升级重新部署

skevy
2018-05-07

智能合约第二种，其他合约账户触发，有什么例子呢

展开

黄威
2018-05-06

期待下一篇實例的講解,抽象還是弄不清楚智能合約。

展开

作者回复: 已经有啦，谢谢支持。

W_T
2018-05-04

请问eos的账户设计是否参考了eth，分为真人账户和合约账户两种

展开

作者回复: 我认为是的，你可以去测试网确认一下。