摘要： 以太坊既是一条以工作量证明为共识机制的公链，也是一个应用平台，能够运行比较复杂的智能合约以及基于合约的app，同时还是一种加密货币，用以支付以太坊公链调用合约时的手续费。因为有了智能合约的加持，以太坊拥有了操作系统级别的想象空间。

我们常常听到人们对于区块链发展时期的划分。以比特币的出现定义区块链1.0时代，以太坊的出现定义区块链2.0时代。比特币在整个区块链世界里，扮演了价值存储的功能，所以被称为数字黄金，而以太坊的出现则定义了智能合约的时代。

如何准确的定义以太坊？笔者认为以太坊在区块链世界中扮演了三个角色：它是一条以工作量证明为共识机制的公链，采用与比特币不同的抗ASIC挖矿算法，计划转为POW+POS Hybrid，名为Casper的共识算法；它是一个应用平台，具有几乎图灵完备的计算能力，能够运行比较复杂的智能合约以及基于合约的app；它同时又是一种加密货币，用于支付在以太坊公链调用合约和记录数据时产生的手续费；

之所以说以太坊开启了一个时代，是因为它使得基于区块链技术构建生态成为可能。美国SEC曾经定义所有的数字货币，本质上可以分为两类，一类是security token，一类是utility token。前者指有融资功能的数字货币，后者指有实际效用的数字货币。由于大部分区块链项目离落地应用非常遥远，所以大多数数字货币属于security token。而这一景象主要归功于以太坊的问题，我认为，以太坊从去年到今年初的暴涨也主要由于它解决了一个极为刚需的问题——中小企业的融资问题。

今天我们就以ERC20代币为例从技术层面来深入解读一下以太坊智能合约。智能合约是1990s年代由尼克萨博提出的，由于缺乏可信的执行环境，一直没有得到实际应用。区块链技术出现后，人们发现区块链天生可以喂智能合约提供可信的执行环境。以太坊的创始人Vitalik最早看到了区块链与智能合约与区块链的契合，发布了《以太坊：下一代智能合约与去中心化应用平台》。

我们知道，区块链的本质是一个分布式账本系统，在比特币网络里，区块里记录的主要是比特币的转账交易信息。而在以太坊的区块中，记录的除了转账信息以外，还有可执行的代码。

首先，我们需要了解一个很重要的概念，叫做EVM（Ethereum Virtual Machine），也就是以太坊的虚拟机。以太坊的每个节点都会运行虚拟机，它不仅能够执行代码，还可以读写区块中可执行的代码和数据，校验数据签名等等。如果把比特币比喻成功能手机，以太坊就像是智能手机。

在以太坊中，有两种账户，一种叫外部账户，是人操作的正常账户，地址即公钥，由私钥控制；一种叫合约账户，地址随机产生，有点像游戏中的NPC（非玩家控制角色，non-player character）。

在外部账户发起并且改变区块链上数据的行为叫交易，比如转账、部署合约和调用合约等等；与之相对应的是查询，指仅仅查看链上的数据而不改变，这种操作并不消耗gas。

那么什么叫智能合约呢？简而言之，智能合约指能够在EVM上运行的代码和数据，是区块链系统的内部应用，拥有自己的账户地址和存储空间。外部账户可以部署智能合约，通过向合约地址提交一笔交易即可调用合约。而合约一旦部署，所有节点都会自动执行，并对执行结果进行验证。同样，智能合约本身是代码，无论是代码还是数据都具有可追溯、一致性、不可篡改的特点，即使是合约创建者也无法对代码进行改动。

目前来说，最受欢迎的智能合约开发语言是Solidity，编译为字节码后部署到主网，通过外部账户发送转账进行调用。经过实测，大家可以尝试发布一个token玩玩。推荐步骤如下：

1. 用MetaMask新建一个以太坊钱包

2. 钱包选择以太坊测试网络Ropsten

3. 用测试网络获取eth

4. 用Remix进行编码和编译

5. 用MEW进行合约部署

6. 用EtherScan进行交易跟踪和合约浏览

因为有了智能合约的加持，以太坊拥有了操作系统级别的想象空间，也是目前来说生态最好的公链，因为它找到了自己的强应用场景。回归到行业本身，虽然我们在开头提到了区块链的1.0与2.0时代，但整个行业依然处于非常早期，我们完全也可以说现在是0.1与0.2时代。

作为一个区块链行业的从业者，笔者认为之所以有必要科普区块链技术，正是为了明晰区块链技术的边界。区块链本身作为一种高冗余的数据存储方式，以牺牲系统效率为代价提升安全性等等，并不是天生适用于所有的应用场景。对于所有公链来说，在未来一段时间的寒冬里，有充足的耐心去解决现有的区块链技术痛点以及培育生态才是真正不辜负这个时代。