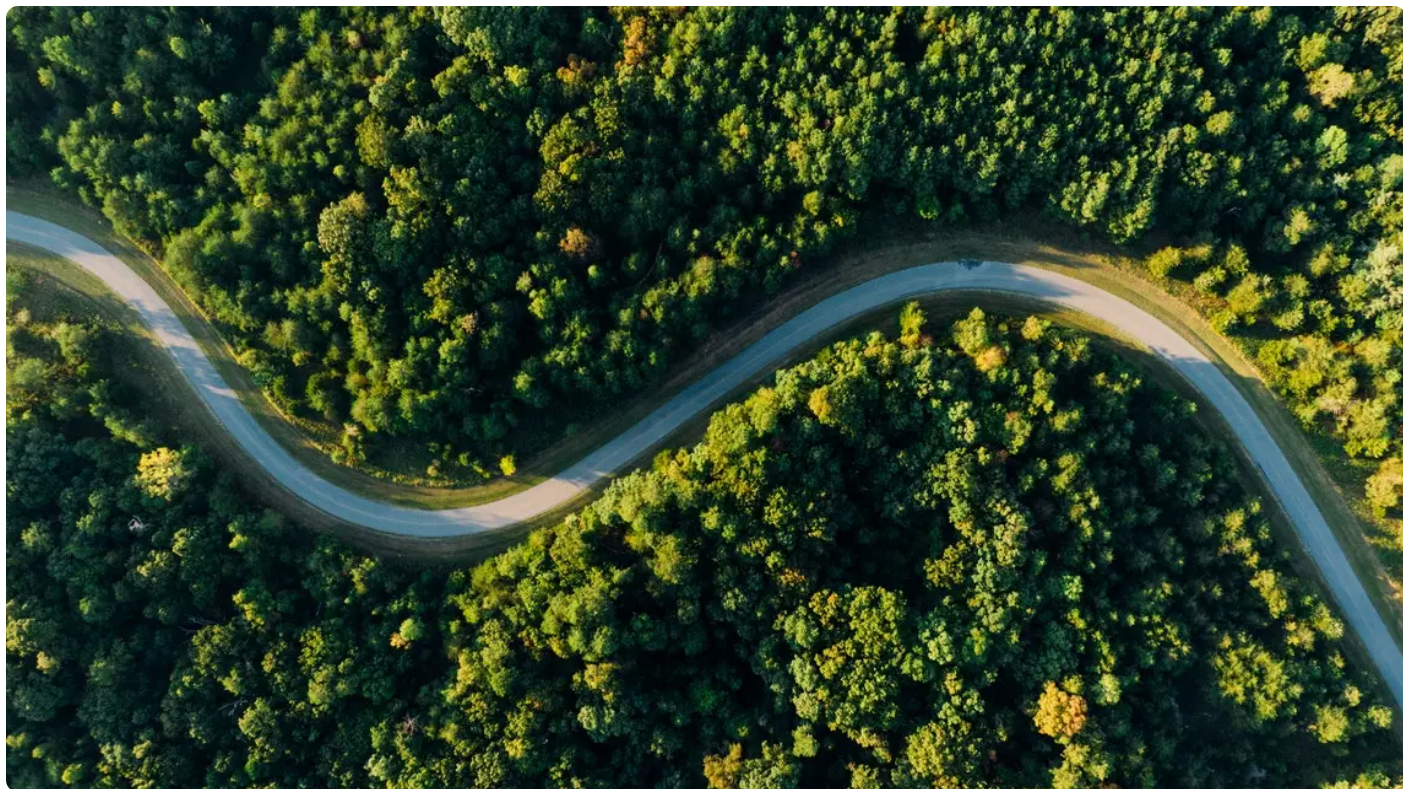


## 09 | 数字交易协议：在数字空间“复制”社会经济活动

2022-05-16 方军

《说透元宇宙》

课程介绍 >



讲述：山荣

时长 19:07 大小 17.51M



你好，我是方军。

这节课，我们接着讨论价值互联网的相关技术与应用。在上一讲，我们看到，区块链技术用巧妙的方式在协议层实现了“账户、余额与转账”，让价值互联网成为可能。

我们希望通过价值互联网实现各种各样的经济互动：我们可以通过支付软件和电商平台付钱给商家；我们可以在数字空间中工作，按照贡献自动获得工资、期权或其他形式的奖励；我们可以拥有会员卡，拥有进入特定俱乐部的权利。

但要注意啊，要把实体世界中的各种经济活动都搬到数字空间，只有上一讲我们说的“账户、余额、转账”功能是不够的。

比方说，如果一个公司使用上一讲我们提到的技术系统，那么，它就只能有一种余额，你用它处理工资，就无法同时用它处理员工期权。又比如，你想给某个员工发一个五周年贡献“金

条”，它做不到，因为它还没有办法处理这类所谓不可互换的财产。另外，在这样的系统上进行应用程序开发也有种种局限性。总之，如果只有上一讲的那种技术系统，我们将实体世界的经济活动映射到数字空间的能力是有限的。

要在数字世界复制人类社会的经济活动，这套技术基础设施还要经过好几轮演化，它包括可编程能力的扩展、进行价值表示的行业事实标准的出现以及交易协议的出现。接下来，我们一步步拆解一下。

## “世界计算机”的诞生：智能合约程序的出现

区块链发展的第一个阶段，是用去中心化网络、分布式账本的方式实现了一个“世界账本”，这个账本可以实现财产所有权系统的三个核心要素：账户、余额、转账。这是一个大突破，但要让这个技术系统更加实用，人们首先遇到的一大障碍是，它没有提供好的计算环境，应用开发者不能自由开发与运行各种各样的程序。

有了问题，就会有人寻找答案，又一个技术创新者出现了。这个创新者是以太坊创始人维塔利克·布特林，他撰写了一篇重要论文叫《以太坊：智能合约和去中心化应用的下一代平台》，而论文最终演变出来的产品就是可以运行智能合约程序的价值计算平台。

在这篇论文中，布特林简洁而精准地定义了第一代区块链系统（比特币系统）。他将区块链系统定义为我们上节课提到的“交易驱动的状态机”。但它的灵活性较小，因为驱动它从一个状态到下一个状态的交易是高度受限的。因此维塔利克提议，建立以太坊区块链，也就是通常所说的第二代区块链，以太坊区块链可以用更容易编程的交易取代原来的交易，这些程序代码运行在以太坊虚拟机（EVM）上。

以太坊虚拟机又是什么呢？

在我看来，以太坊虚拟机有点像 CPU 芯片，我们可以用高级语言编写程序，然后将程序编译成字节码在这个 CPU 上运行。有了虚拟机的设计，应用开发者就有了完备的计算环境，我们可以在上面开发各种各样的应用了。

以太坊的理念得到了一群人的支持，其中有一个重要人物就是加文·伍德，他是以太坊的 CTO。加文·伍德完成了以太坊技术规范文档也就是《以太坊黄皮书》的撰写，他旗下的团队完成了以太坊重要的软件客户端 Parity 的开发，加文·伍德也是我们现在常用的智能合约编程

语言 **Solidity** 的主要开发者。在离开以太坊之后，加文·伍德还创办了 **Web3 基金会**，推出了以跨链为特征的波卡区块链系统。

我们讲了这么多加文·伍德的成就，是想引出他对以太坊的一个关键设想。在开发出以太坊虚拟机，设想以太坊的各种可能性时，他给以太坊下了一个特别响亮的定义：以太坊就是“世界计算机”。

这是一个精彩的提法，第一代区块链实现了所有权管理系统最基础的部分，也就是“世界账本”。但作为一个技术系统，只是相对静态的账本是远不够的。现在，**在第一代区块链账本的基础之上，以太坊增加了应用代码运行的环境，自此，区块链变成了“世界账本 + 世界计算机”。**

当然了，“世界计算机”更像一个营销用词，在区块链技术行业，大家常用的是一个更平实、也更准确的词——**“智能合约平台”（Smart Contract Platform）**。以太坊区块链开创了这一类别，并且目前是这一类别中规模最大的。特别说一下，普通人听到智能合约这个词，可能会觉得它就是商业社会中的合约或协议，但其实，它真正指的是程序，是区块链上运行的独特的服务端程序。

智能合约平台，就是运行这些独特的服务端程序的计算平台。从区块链技术发展迭代的角度看，它是在实现了“账户、余额、转账”三个功能的账本系统的基础之上，增加了一系列新的组件，让我们可以编程、处理更加复杂的操作。具体来说，以太坊中的新组件包括三个部分。

第一是运行代码的计算环境，还有和运行环境对应的数据存储机制，这些被统称为以太坊虚拟机。

第二是可以运行在以太坊上的特定程序，也就是智能合约程序。我们把智能合约代码编译、部署到链上后，它就成为了合约账户。与我们熟悉的服务端程序不同，智能合约在部署后，其代码不可修改。此外，合约也不会自动运行，相当于处于待机状态，只能被外部触发运行。

第三是高级编程语言、开发工具和更便于使用的以太坊钱包。有了这些之后，在区块链上进行应用开发就方便了许多。

我们知道，在数字世界中，一切都是由代码组成的。区块链技术发展到这个阶段，有了虚拟机、智能合约程序、开发工具，我们开发各种各样价值互联网应用的空间就被彻底打开了。

## 可互换与不可互换通证标准

要让区块链成为广泛适用的财产所有权管理系统，还需要再往前走一步。接下来，我们一起来看看通证标准。从编程角度看，通证标准是智能合约程序的接口标准化。我们先来看看通证这个新东西是什么意思。

**通证（Token），就是数字空间中财产所有权的凭证。**2017 年底，有人把 Token 翻译成通证，这很贴切。在实体世界中，我们手上的钱、我们的股权合同、我们的房产证都是某种财产所有权的凭证。通证，是这些财产所有权凭证在数字空间的对应物，是数字版的所有权凭证。

通证主要分为两种：可互换通证与不可互换通证。如果我和你持有的是同一家公司的股票，每股股票的价格是相等的、可互换的，这类所有权凭证用“可互换通证”来表示。但是，如果一个女生有一只 LV 包，但即便是另一只同一款式的 LV 包，跟她自己的这一只也有着不同的“记忆”，二者是不可互换的，这类所有权凭证要用“不可互换通证”来表示。

对应地，也就出现了两种通证标准，它们在以太坊生态内分别是第 20 号和第 721 号改进提案，因此常被称为 ERC20 标准和 ERC721 标准。由于 2021 年 NFT 头像、艺术及国内数字藏品的爆火，不可互换通证的缩写——NFT（non-fungible token）——现在也广为人知。

为什么要提出“通证标准”并让它们成为行业中的事实标准呢？我们以“可互换通证”为例来看看。

**我们先从财产凭证的角度来看。**假设我们生活在一千年前的欧洲，那是一个用金子作为货币的时代，在大家没有广泛接受金币之前，商人们只能用称去称金子的重量。但在有了佛罗伦萨的弗罗林金币（forlin）和威尼斯的达克特金币（ducat）之后，商人们就可以很方便地用这些货币来做生意了，在商业流转中，金币比金子更便捷。可以说，区块链上的通证标准也是基于同样的需求被创造出来的。

要注意的是，区块链上的通证可以表示很多东西。除了金钱之外，它可以用来表示商场的积分，可以表示我们累积的航空里程，可以用来表示员工期权。任何有价值的事物的所有权，都可以用通证来表示。

以上所说的这一类财物的共同点是，它们可以切分到最小单位，每个最小单位都是可互换的。以航空里程为例，里程以余额的方式被记录下来，今天的一公里里程和昨天的一公里里程是可以互换的。这正是为什么 ERC20 被称为“可互换通证”。

**我们再从软件编程的角度来看一下。**要让各种程序都能方便地处理不同的可互换通证，这些通证最好遵循一致的标准，也就是，它们应该提供同样的编程接口供其他程序调用。

以 **ERC20** 通证标准为例，我们以一个人的地址为输入参数、调用 **balanceOf()** 函数，可以知道这个人拥有的数量；我们调用 **transfer()** 函数，输入相应的输入参数，可以把一个人的通证转给另一个人。另外，通证标准还要求，在这些函数发生调用、变更所有权信息时，它也应该发出事件（**event**），供外部程序监听事件、做出相应的处理。

遵循标准的编程方式优点很明显。只要你按照标准提供接口，别的应用程序就可以按标准来调用，不用管你内部的实现细节。

2015 年底，**ERC20** 标准被提了出来，现在，它已经成为了区块链业界的事实标准。虽然它的名字实际意思是“以太坊改进提案第 20 号”，其实，在以太坊生态之外，绝大多数区块链也遵循这一标准。

但有这一种可互换通证（也就是 **ERC20** 通证）就够了吗？不够。仔细观察我们周围的实体世界，你会发现，能够被折算成数字进行统计的财物是少数，绝大部分财产是不可互换的。比如，这所房子和那所房子不可互换，你的两件衣服之间不可互换，你的手机和别人的手机也不可互换……我可以一直列举下去。

在数字空间，可互换的财物也是少数，不可互换的财物同样普遍。2018 年初，有人提出要建立所谓不可互换通证的标准，这就是 **ERC721** 提案，它建议把这一类财物所有权凭证的编程接口也标准化。现在看到的绝大部分 **NFT** 头像、艺术品、游戏道具都遵循 **ERC721** 标准。

有了 **ERC20** 和 **ERC721** 这两大类通证标准之后，区块链技术作为一个财产所有权管理系统就进化到了一个新的阶段。

我们可以把这种财产所有权管理系统类比成一家美国的银行，我们来看看这一家“银行”的升级换代。

最初，这家银行只能管理美元这一种货币。有了 **ERC20** 可互换通证标准之后，它的系统就可以同时管理日元、欧元、港币等各种货币了，它还可以管理成千上百家上市公司的股份。而有了 **ERC721** 不可互换通证标准之后呢，这家银行又有了新能力，它可以帮客户管理艺术收藏品、房产所有权、未上市公司股权等等财产，这些财产是两两不可互换的。

因此，在有了这两种通证标准之后，区块链从单一的财产所有权管理系统，演变成了全功能的财产所有权管理系统。我们也可以说，各种各样的价值都可以在用区块链技术构建起来的价值网络中流转了。

再回看区块链技术到这里的发展过程，我们看到，它已经经历了三个阶段。

第一阶段，用“区块 + 链”的数据结构、用“去中心网络 + 分布式账本”的方式形成了财产所有权管理系统的技术雏形。这一阶段实现了所有权管理系统最核心的“账户、余额、交易”三要素。

第二阶段，为区块链账本增加了代码运行环境，放在以太坊生态内来说就是，增加了“以太坊虚拟机”，为编程与应用开发提供了可能性。

第三阶段，行业形成了一些标准程序接口，主要是 **ERC20** 可互换通证标准和 **ERC721** 不可互换通证标准等。到这里，在区块链技术支撑的价值互联网中，我们可以方便地表示各种类型的价值，并进行价值的流转了。

## 交易协议：将人类经济活动全面映射到数字空间

有了这些技术准备之后，我们可以尝试着将一些人类经济活动映射到数字空间了。这带来了区块链技术发展的第四阶段，也就是交易协议阶段。

**协议（Protocol）是区块链领域的专业术语，指的是由一组智能合约组成、运行在区块链上、由用户与之交互的功能组合。**它与现在我们熟悉的互联网平台所说的“平台”有所不同。平台是由某个公司运行与掌控的，其权益属于一家公司，而协议是众人一致同意、共同遵守的规则，而其权益属于所有参与者。

为了便于理解，我还是切换到我们熟悉的场景来类比解读，我们以一类典型的协议为例。

打个比方，在数字空间中，我因为参与了创业项目并努力工作、做出贡献，获得了价值 10 万美元的通证奖励。但我拿到的通证奖励有个限制条件：除非得到“公司”的书面许可，否则我不能卖掉它们。有一天，我发现了一个很喜欢的 **NFT** 头像，我想用 10 万美元买下来当成传家宝。这时，我就需要一种实体世界里常见的服务：抵押、借贷。

区块链上的确出现了一类名为“借贷协议”（**Lending Protocol**）的服务，相应的产品有 **Compound**、**AAVE** 等。它们的运作原理是，接受某些通证作为抵押，让用户借贷资金。再具



体拆解一下，这一类协议实际上是由两个服务组合而成的：第一，我将通证存进去，我按照一定的利率获得利息收入；第二，我抵押它、获得贷款，我要支付贷款利息。贷款利息与存款利息之差，就是我付出的成本。另外，如果我的通证跌价、抵押物不足，我会有被清算的风险。

这么讲解借贷协议的原理，你一定觉得很常见，其实它就是零售银行的业务模型。真正有意思的是这个逻辑用区块链技术实现的方式。

**第一，与传统的零售银行有很多员工不同，借贷协议无须人工参与，由用户自行与区块链上的相关智能合约程序交互。**

- 当我要向它存款时，我自己将通证存入它的一个智能合约。
- 当我决定要抵押时，审计官合约会进行计算，告诉我在它的整个系统中，我这个抵押物的价值是多少，可以贷多少钱。
- 当我要借款时，我向它的另一个智能合约发起请求，自己完成借贷。
- 当我去还款时，我还是在跟对应的智能合约交互，存入要归还的贷款和利息，取出自己的抵押物。

**第二，这些智能合约是自主运行的，它们拥有自主权，可以独立、公正地替我们所有人保管资产。**资产是完全由智能合约也就是代码管理的，没有人能偷偷地动用这些资产。类比来说，一个大股东想把钱偷偷地抽走是不可能的。当然，这一切的前提是，程序员没有偷偷地给自己留后门，我们可以通过审核智能合约代码来规避这种行为。

智能合约程序组成的协议，它的工作原理有点像街头的自动饮料售货机。它一开始处在静止状态，我们扔进去硬币、选择饮料，罐装饮料落到取货筐中。我们外部的购买行为，触发它从一个状态变化到了另一个状态。之后，它又停在了那个状态，直到再次被交易触发。售货机在街头替它的主人自主地管理内部的硬币和饮料。

在区块链上，我们编写各种类型的智能合约，就可以实现各种各样的“自动售货机”。除了借贷协议，我们还可以实现积分、兑换、抽奖等功能。当然，你也可以用智能合约实现更复杂的金融应用，或用智能合约实现与金融完全无关的交易类应用。它们背后的技术实现逻辑都是相似的，依赖智能合约程序的特性来完成交易。

现在在各种区块链中，可能有上万种交易协议在运行着，它们的特点可以总结为以下三点。

第一，一个协议是部署在区块链上的一组智能合约，这些合约组合起来实现了某种业务逻辑，它通常是实体世界中人类经济某种活动的翻版。

第二，协议处理的主要是用通证表示的财产。这些通证既可以是可互换通证，也可以是不可互换通证。它能够接受通证，保管通证，给出通证。这是它和现在互联网上绝大部分应用的关键区别。当前互联网上的应用多数是处理信息，而这些协议处理通证则代表着在处理价值。

第三，这组智能合约是自主运转的程序体，它们会保持在某种状态，直到有用户与它交互时，它才会被触发，按预设的业务逻辑处理用户的需求。

当然，每个协议的自主程度有所不同。在下一讲中，我们会重点讨论人们如何管理这些协议。

## 总结

小结一下。在这一讲中，我们将区块链技术进化分成四个阶段。我们再一起来整体回顾一下。

第一阶段，区块链技术诞生了，我们拥有了“区块 + 链”的账本结构，它可用作财产所有权管理系统。

第二阶段，以太坊为区块链增加了代码运行的环境，让我们可以编写名为智能合约的独特的服务端程序。

第三阶段，表示两种类型财产所有权的接口标准被确立了，可互换与不可互换通证标准让所有的财产都可以用通证表示出来。

第四阶段，将人类经济活动映射到数字空间的交易协议产品开始出现、并大爆发。

第四阶段的创新主要是在 2020-2022 年这三年间出现的。有了技术基础设施，相当数量的用户进入了区块链领域，大量的数字交易协议就在这个阶段就被创造出来了。当然，我们也必须承认，从长远来看，目前这些交易协议产品多数仍处于早期试错阶段。但不管怎样，到了这个阶段，价值互联网的技术基础构建就基本完成了。在下一讲，我们会讨论价值互联网的另一个关键模块“数字治理协议”。它的难点将不再是技术，而是人与人之间的协同与合作。


## 课后题



最后，我给你留一道思考题。刚才，我们介绍了数字交易协议，在你看来，现实世界有哪些比较复杂的经济活动可以用数字交易协议来实现？欢迎在留言区说出你的想法。

分享给需要的人，Ta订阅超级会员，你最高得 50 元

Ta单独购买本课程，你将得 20 元

 生成海报并分享

 赞 1  提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 08 | 数字财产确权：用区块链建立数字所有权管理系统

下一篇 10 | 数字治理协议：数字世界中的人如何组织与大规模协作

## 精选留言 (2)

 写留言



rondo

2022-05-16

区块链之间的交易现阶段是不是还要受到各国法律框架的制约？



peter

2022-05-16

请教老师一个问题：  
现在市面上有实用的AI唱歌软件吗？就是能用该AI唱所有歌曲。

