

## 4.3以太坊虚拟机EVM

**虚拟机：**实际上不是物理计算机，而是一个**用来模仿物理计算机的软件环境**，但虚拟机可以像物理计算机一样运行程序。用于托管虚拟机的物理计算机通常可以支持多台虚拟机。另外，不仅在系统层上有虚拟机的概念，**在程序语言上也有虚拟机的概念**，比如 java 的 JVM，微软的 .NET 等。

## 虚拟机是用来解决什么问题呢？

为了抽象掉硬件底层。从系统层来说，硬件和操作系统都越来越多样化了。比如同样是X86的CPU，有的支持到SSE4，有的只支持MMX，还有的只支持3DNow，如果想要代码跑得快，需要自己去做繁琐的检测，还要写多份代码来应对。如果其他硬件也出现了各种不同，例如硬盘接口SCSI、IDE、SATA、iSCSI，3D运算DirectX、OpenGL、3dfx等等，会产生更多不便。于是虚拟机就诞生了，它可以自动兼容所有硬件。

虚拟机技术基本上都是将硬件层或是系统层进行了一次抽象，以致对应用层屏蔽掉了底层的实现细节，**有利于应用的快速实现和部署。**

虚拟机按层次来说可以分为下列三大类：**高级语言虚拟机、操作系统层的虚拟机和硬件层的虚拟机**

- 然而它们的实现越往底层难度就越大。
- 对于一个操作系统，它们的架构层次是：最下层是硬件层，之上是硬件驱动，再之上是操作系统内核，然后才是操作系统接口和应用程序。我们可以把任何形式的虚拟机都想象成一个容器，在这个容器里它截获了本该发往底层的指令，自己处理。
- **高级语言虚拟机**：是就一个代码解释器，不需要二进制代码，只需要中间代码，然后虚拟机处理后，再移交给 CPU 和存储结构。虚拟机模拟的是代码的执行。
- **操作系统层的虚拟机**：所有操作系统接口调用都会被该容器截获，经过处理后，发送到当前适当的平台上。
- **硬件层的虚拟机**：是最复杂的工程，是虚拟化技术的一大重点，是对硬件层以及硬件驱动层的模拟。

### 区块链怎么支持各个领域的业务逻辑呢？

- 传统的精简指令集计算机的 CPU 只提供了有限的执行指令和存储器，但是各种类型的应用都能在这台计算机上运行。究其原理，就是因为系统存在一个“虚拟机”将高层语言的实现都转换成了 CPU 的相关执行指令。高层语言提供语法，人们使用高级语言开发相关应用。由低到高的层次结构分别为：硬件指令，虚拟机，高级语言和应用层。
- 很明显，如果要在区块链里支持各种应用，也需要有这样的层次结构，因此需要区块链提供一套指令，并且区块链里的虚拟机可以对这些指令作相关的解释。另外，高级语言的实现需要有一个编译器将实现编译成虚拟机支持的指令。这样，区块链就完美支持了语言和业务的分层，从而可以在区块链里开发各种业务应用。

### 虚拟机架构组织及运行原理

虚拟机架构的组成部分：

- 指令：区块链系统底层支持的原子操作指令
- 虚拟机：对原子操作指令的解释
- 编译器：将高级语言转换为虚拟机支持的指令
- 高级语言：用于实现在区块链里运行业务应用

还有两个重要的组成部分

- 1. 区块链系统提供的原始 API，用于在编写智能合约需要时，获取系统相关数据或是状态；
- 2. ABI，全称是 application binary interface，一个智能合约发布后，其他的应用需要知道这个合约提供了什么功能接口以及数据结构。

### 虚拟机架构组织及运行原理

因此，当所有的部分都就绪后，我们就可以用**高级语言和 API 编写符合业务逻辑的智能合约**，**然后用相关编译器将智能合约编译成 byte codes**，**并且也会生成相关的 ABI 描述**。经过严格测试后，就可以将智能合约的 byte codes 和 ABI 以交易的形式发布到区块链中。矿工会验证你交易的合法性，如果入块成功，将会返回智能合约地址。用户会调用这个合约地址来获取 ABI，再根据 ABI 里对功能接口的描述来发起一笔对功能接口调用的交易，从而实现相关功能或是获取相关结果。矿工同样也会这笔交易进行合法性验证及入块处理。

- 我们可以使用 solidity 编写智能合约，使用 remix 编译调试智能合约。将经过严格测试的智能合约代码发布到区块链上，可以理解为一个特殊的交易——包括了可执行代码的交易，然后会被矿工记录在某个块中。当需要调用这个智能合约时，只需向这个智能合约的地址发送一个交易即可。因为每个节点都需要安装以太坊客户端，而每个客户端都自带了一个 EVM (以太坊虚拟机)。通过交易触发智能合约后，智能合约的代码就能在 EVM 上被执行。这种方式**相当于把程序部署到了很多的电脑上，随时都可以通过交易来触发这些智能合约的执行**，从而也完成了去中心化程序的部署和调用。
- **以太坊的 EVM 不仅支持转账类型的业务，它还可以应用到很多传统的行业**，比如投票、公正、版权、医疗。DAPP 就是基于以太坊运行的去中心化应用，这种应用涉及到传统行业的方方面面。