

## 以太坊

(英文Ethereum)是一个开源的有智能合约功能的公共区块链平台,通过其专用加密货币以太币(Ether,简称“ETH”)提供去中心化的以太虚拟机(Ethereum Virtual Machine)来处理点对点合约。

以太坊的概念首次在2013至2014年间由程序员Vitalik Buterin受比特币启发后提出,大意为“下一代加密货币与去中心化应用平台”,在2014年通过ICO众筹开始得以发展。

截至2018年2月,以太币是市值第二高的加密货币,仅次于比特币。

中文名以太坊外文名Ethereum

属性平台创始人杰弗里·维尔克

## 产生背景

比特币开创了去中心化加密货币的先河,五年多的时间充分

图1.ETF检验了区块链技术的可行性和安全性。比特币的区块链事实上是一套分布式数据库,如果再在其中加进一个符号——比特币,并规定一套协议使得这个符号可以在数据库上安全地转移,并且无需信任第三方,这些特征的组合完美地构造了一个货币传输体系——比特币网络。

然而比特币并不完美,其中协议的扩展性是一项不足,例如比特币网络里只有一种符号——比特币,用户无法自定义另外的符号,这些符号可以是代表公司的股票,或者是债务凭证等,这就损失了一些功能。另外,比特币协议里使用了一套基于堆栈的脚本语言,这语言虽然具有一定灵活性,使得像多重签名这样的功能得以实现,然而却不足以构建更高级的应用,例如去中心化交易所等。以太坊从设计上就是为了解决比特币扩展性不足的问题。

## 设计原则

编辑

简洁原则

以太坊协议将尽可能简单,即便以某些数据存储和时间上的低效为代价。一个普通

的程序员也能够完美地去实现完整的开发说明。这将最终有助于降低任何特殊个人或精英团体可能对协议的影响并且推进以太坊作为对所有人开放的协议的应用前景。添加复杂性的优化将不会被接受，除非它们提供了非常根本性的益处。

## 通用原则

没有“特性”是以太坊设计哲学中的一个根本性部分。取而代之的是，以太坊提供了一个内部的图灵完备的脚本语言以供用户来构建任何可以精确定义的智能合约或交易类型。想建立一个全规模的守护程序（Daemon）或天网（Skynet），你可能需要几千个联锁合约并且确定慷慨地喂养它们，一切皆有可能。

## 模块化原则

以太坊的不同部分应被设计为尽可能模块化的和可分的。开发过程中，应该能够容易地让在协议某处做一个小改动的同时应用层却可以不加改动地继续正常运行。以太坊开发应该最大程度地做好这些事情以助益于整个加密货币生态系统，而不仅是自身。

## 无歧视原则

协议不应主动地试图限制或阻碍特定的类目或用法，协议中的所有监管机制都应被设计为直接监管危害，不应试图反对特定的不受欢迎的应用。人们甚至可以在以太坊之上运行一个无限循环脚本，只要他愿意为其支付按计算步骤计算的交易费用。

## 功能应用

### 编辑

以太坊是一个平台，它上面提供各种模块让用户来搭建应用，如果将搭建应用比作造房子，那么以太坊就提供了墙面、屋顶、地板等模块，用户只需像搭积木一样把房子搭起来，因此在以太坊上建立应用的成本和速度都大大改善。具体来说，以太坊通过一套图灵完备的脚本语言（Ethereum Virtual Machinecode，简称EVM语言）来建立应用，它类似于汇编语言。我们知道，直接用汇编语言编程是非常痛苦的，但以太坊里的编程并不需要直接使用EVM语言，而是类似C语言、Python、Lisp等高级语言，再通过编译器转成EVM语言。

上面所说的平台之上的应用，其实就是合约，这是以太坊的核心。合约是一个活在以太坊系统里的自动代理人，他有一个自己的以太币地址，当用户向合约的地址里

发送一笔交易后，该合约就被激活，然后根据交易中的额外信息，合约会运行自身的代码，最后返回一个结果，这个结果可能是从合约的地址发出另外一笔交易。需要指出的是，以太坊中的交易，不单只是发送以太币而已，它还可以嵌入相当多的额外信息。如果一笔交易是发送给合约的，那么这些信息就非常重要，因为合约将根据这些信息来完成自身的业务逻辑。

合约所能提供的业务，几乎是无穷无尽的，它的边界就是你的想象力，因为图灵完备的语言提供了完整的自由度，让用户搭建各种应用。白皮书举了几个例子，如储蓄账户、用户自定义的子货币等。

## 发展历史

### 编辑

2013年年末，以太坊创始人Vitalik Buterin发布了以太坊初版白皮书，启动了项目。2014年7月24日起，以太坊进行了为期42天的以太币预售。2016年初，以太坊的技术得到市场认可，价格开始暴涨，吸引了大量开发者以外的人进入以太坊的世界。中国三大比特币交易所之二的火币网及OKCoin币行都于2017年5月31日正式上线以太坊。 [1]

自从进入2016年以来，那些密切关注数字货币产业的人都急切地观察着第二代加密货币平台以太坊的发展动向。

作为一种比较新的利用比特币技术的开发项目，以太坊致力于实施全球去中心化且无所有权的数字技术计算机来执行点对点合约。简单来说就是，以太坊是一个你无法关闭的世界计算机。加密架构与图灵完整性的创新型结合可以促进大量的新产业的出现。反过来，传统行业的创新压力越来越大，甚至面临淘汰的风险。

比特币网络事实上是一套分布式的数据库，而以太坊则更进一步，她可以看作是一台分布式的计算机：区块链是计算机的ROM，合约是程序，而以太坊的矿工们则负责计算，担任CPU的角色。这台计算机不是、也不可能是免费使用的，不然任何人都可以往里面存储各种垃圾信息和执行各种鸡毛蒜皮的计算，使用它至少需要支付计算费和存储费，当然还有其它一些费用。

最为知名的是2017年初以摩根大通、芝加哥交易所集团、纽约梅隆银行、汤森路透、微软、英特尔、埃森哲等20多家全球顶尖金融机构和科技公司成立的企业以太坊联盟。而以太坊催生的加密货币以太币近期又成了继比特币之后受追捧的资产。

## 项目争议

## 编辑

以太币在中国生根落地，引得市场纷纷侧目，然而在价格已经创下历史新高的时刻，以太币的到来，国外的学者已经指出在整个以太币的智能合约交易中，10%是庞氏骗局，也就是说有人在借以太坊平台发融资项目获得资金，而以太币则成为一种媒介，这些融资项目可能只是一个画饼的计划。看似公平的以太坊众筹，其实是完全不等额的现实货币融资，别人的以太币成本是300元，你的以太币成本是1800元，然后抱团一起做一个项目。而所谓的30%盈利率其实是在庄家市值盈利600%的基础上的盈利，最后托盘的便是以高市值入场的接盘侠。

市场人士指出，以太坊平台上的众筹项目还存在诸多风险，首先以太币不是去中心化数字货币，存在巨庄而且持有80%以上的市值，一直未动，相当于每一个币民头顶都悬着一把利刃；其次以太坊的众筹货币分4-5轮进行解禁，需要变现，所以众筹的项目越多，解禁的压力越大；第三众筹基金的融资效应，每一次众筹都需要十倍百倍的以太坊数字货币等待融资，而不是参与交易，众筹结束后这部分货币重新进入市场进行打压；第四众筹基金的参与获利，众筹基金的目的便是获利，融到以太币不是积极参与众筹而是抛售，然后等待市值下降的时候购入再返还给用户，这便是标准的“做空获利”；第五以太坊所有的众筹项目都没有确立以太坊的货币地位，而是以积分、交易税费的形式进行抵扣，也就相当于淘宝币、天猫积分一样的性质，可抵用但是永远无法取代货币的功用。

值得关注的是，在2017年6月美国科技股大跌的时候，以太币在创下407美元/个新高之后，截至6月15日，其价格也跟随美国科技股连续出现下跌，跌幅达到15%。