以太坊

以太坊简介

以太坊是一条区块链，其中嵌入了计算机。 它是以去中心化、无需许可、抗审查的方式构建应用程序和组织的基础。

在以太坊宇宙中，有一台规范化计算机（称为以太坊虚拟机，或 EVM），其状态得到以太坊网络中所有人的一致同意。 每个参与以太坊网络的人（每个以太坊节点）都会保存一份该计算机的状态。 此外，任何参与者都可以广播请求这台计算机进行任意计算。 每当广播这样的请求时，网络上的其他参与者就会检查、验证并进行（“执行”）该计算。 该执行会导致以太坊虚拟机的状态变化，并且在整个网络中传播。

计算请求被称为交易请求；所有交易的记录以及以太坊虚拟机的当前状态存储在区块链中，而区块链又由所有节点存储并达成一致。

加密机制确保一旦交易被验证为有效并添加到区块链中后，之后就无法被篡改。 同样的机制还确保所有交易都以适当的“权限”签名和执行（除了 Alice 本人，任何人都不能从 Alice 的帐户发送数字资产）。

以太坊采用权益证明共识机制。 任何想在链上添加新区块的人都需要往存款合约里至少质押 32 个以太币并运行验证者软件。 然后，他们会被随机选择去提议区块，其他验证者检查区块并将其添加入区块链。

以太币 (ETH)

以太币 (ETH) 是以太坊上的原生加密货币(相同概念的有比特币)。 以太币的目的是允许计算市场化。 这种市场为参与者提供了一种经济激励，以验证并执行交易请求，为网络提供计算资源。

任何广播交易请求的参与者还必须向网络提供一定数量的以太币作为奖金。 网络将把这种奖金奖励给最终验证交易、执行交易、将其提交到区块链并广播到网络的任何人。

支付的以太币数量对应于进行计算所需的时间。 这类奖励也可以防止恶意参与者通过请求执行无穷计算或资源密集型脚本来故意堵塞网络，因为这些参与者必须为自己的计算时间付费。

以太币还用于通过以下三种主要方式为网络提供加密经济安全性：1) 作为一种奖励方式，奖励提议区块或指出其他验证者不诚实行为的验证者；2) 由验证者抵押，作为遏制不诚实行为的抵押品 — 如果验证者试图行为不端，它们的以太币可能会被销毁；3) 用于对新提议的区块的“投票”进行加权，并影响共识机制的分叉选择部分。

智能合约

实际上，参与者不会每次在以太坊虚拟机上请求计算时都编写新代码。 相反，应用程序开发者将程序（可重用的代码片段）上传到以太坊虚拟机状态，用户发出请求以使用不同参数执行这些代码片段。 我们将这些上传至网络并由网络执行的程序称为智能合约。

简单来说，你可以把智能合约想象成一种自动售货机：通过特定参数调用脚本后，如果满足某些特定条件，就会执行一些操作或计算。 例如，如果调用者将以太币发送给特定的接收者，简单的卖方智能合约就可以创建和分配数字资产所有权。

任何开发者都可以创建智能合约，并使用区块链作为其数据层，将其公开给网络，但要向网络支付以太币。 然后，任何用户都可以调用智能合约来执行其代码，并再次向网络支付费用。

因此，通过智能合约，开发者可以任意构建和部署面向用户的复杂应用程序和服务，例如市场、金融工具、游戏等