很多人都在一定程度上听说过以太坊，但是你了解以太坊吗？作为区块链技术2.0，以太坊被称为公共链之王(未来可能会有更多赢家)。它的价值从何而来，与区块链1.0有何不同？

自2008年BTC币出现以来，它的存在逐渐被一些人所接受，人们也积极展开了基于BTC的商业应用的思考和开发。然而，随着应用的扩展，人们发现BTC的设计只适用于虚拟货币场景。由于非图灵完备性的存在，缺乏保存状态的账户概念，以及PoW挖掘机制带来的资源浪费和效率问题，在很多区块链应用场景中并不适用。

因此，人们需要一种新的基于区块链的智能合同开发平台，具有图灵完备性、高效的共识机制，支持更多的应用场景。在这种情况下，以太坊应运而生。

以太坊的目的是整合和完善链条上的脚本、竞技币、元协议等概念，让开发者可以创建任何基于共识、可扩展、标准化、图灵完备、易于开发、协作的应用。

以太坊是一个通用的全球区块链，可以管理金融和非金融应用的状态。以太坊的新颖之处在于它神奇的计算机网络，推动了一种新型的软件应用，真正的去中心化应用。将信任逻辑嵌入小程序并在区块链上运行。。与BTC相比，以太坊建立了一个新的密码技术基础框架，使得在其上开发应用更加容易，并且对轻客户端友好。同时，它允许应用程序共享一个可行的分散式应用程序，并打开了大门。从长远来看，它带来的变化将影响全球经济和控制结构。。

以太坊是一种平台和编程语言，包括数字货币以太和以太脚本，用于构建和发布分布式应用。

以太坊ETH与著名的数字货币比特币BTC有很多相似之处。两者都是数字货币，不可伪造，而且都是以去中心化的方式运作，保证货币供应不被一方控制。以太坊的另一个重要特点是提供了完整的编程语言环境。有时称为以太网脚本。编程语言被人类用来控制计算机的工作。因此，用任何编程语言编写的指令对计算机来说都是准确无误的。

从最低的角度来看，以太坊是基于密码学的多层开源技术协议。其不同的功能模块通过设计完全集成。总的来说，它是一个创建和部署分散式应用程序的综合平台。尽管以太坊看起来像是许多相互关联的开源项目的混合物，但是它的发展有着明确的目标，所以所有的组件都可以协同地组装在一起。

以太坊是区块链与智能合约的完美结合，是智能合约的完整解决方案。，设计为通用的去中心化平台，拥有一整套可以扩展功能的工具，在P2P网络、加密、HttpCli

ent等技术的支持下，实现了一个类似于比特币的区块链。它通过工作量证明机制实现共识，矿工挖矿。，通过P2P网络广播协议实现区块链和其他操作的同步。

以太坊和比特币的区别在于，智能合约可以随意写在上面，通过智能合约实现强大的功能，实现去中心化应用的开发。。部署在以太坊的智能合约运行在以太坊特有的虚拟机上，通过以太坊虚拟机和RPC接口与底层区块链交互。

以太坊技术的九大核心概念

1。以太坊虚拟机：EVM

EVM是以太坊智能合约的运行环境。这是以太坊项目的又一重大创新。它是由许多相互连接的计算机组成的。任何人都可以上传程序并自动执行。同时，确保每个程序现在和所有以前程序的状态总是公开可见的。

2。以太坊账户

以太坊有两种类型的账户。它们共享同一个地址空间：外部账户：这类账户相对受公钥和私钥控制；合约账户：此类账户由账户中存储的代码控制。外部帐户的地址由公钥确定。合同帐户的地址是根据合同创建者的地址和创建合同时此地址发送的交易数量计算的。

两类账户的唯一区别是外部账户没有代码，人们可以通过创建和签署交易从外部账户发送消息。。每当契约帐户收到一条消息时，契约内部的代码就会被激活，允许它读取、写入、发送其他消息并创建契约。

以太坊的账号包含四个部分：

a.随机数。用于确定每笔交易只能处理一次的计数器；

B.以太币账户当前余额；

C.账户的合同代码(如有)；

D.账户存储(默认为空)。

3。以太坊消息

以太坊消息在某种程度上类似于比特币交易，但两者有三个重要区别。

1)以太坊的消息可以由外部实体或合约创建，但比特币的交易只能从外部创建；

2)以太网消息可选地包含数据；

3)如果以太坊消息的接收方是合约账户，可以选择回复，这意味着以太坊消息中也包含了函数的概念。

4。以太坊交易

The&quot；交易&quot在以太坊中是指包含从外部帐户发送的消息的签名数据包。该事务包含消息的接收方、用于确认发送方的签名、以太坊账户的余额、要发送的数据以及两个名为STARTGAS和GASPRICE的数值。。为了防止代码出现指数级爆炸和无限循环，每个事务都需要限制执行代码导致的计算步骤。STARTGAS是用需要支付的燃料来限制计算步骤，GASPRICE是每个计算步骤需要支付给矿工的燃料价格。。

5。燃气

以太坊上的每一笔交易都会收取一定量的燃气。设置Gas的目的是限制执行事务所需的工作量，并为事务的执行支付费用。当EVM执行交易时。气体会按照一定的规律逐渐消耗。燃气价格由交易创建者设定，发送账户需预付的交易费用=燃气价格*燃气金额。如果执行后有气体剩余，这些气体将被返回到发送帐户。。无论在哪里执行，一旦气体耗尽，就会触发缺气异常。同时，当前调用框架所做的所有状态修改都将被回滚。

6。存储器、主存和栈

每个账户都有一个永久存储区。称为存储，采用键-值的形式，键和值的长度都是256位。与主存和栈相比，存储的读操作开销很大，一个契约只能读写自己的存储。

第二个内存区域称为主内存。。契约每执行一次消息调用，就有一个新的被清空的主存，可以按字节寻址，但读写的最小单位是32字节。操作主存的成本随着主存的增长而增加。

EVM不是基于寄存器，而是基于栈的虚拟机。。所有的计算都在一个叫做堆栈的区域中进行。你可以将栈中的元素放入存储器或主存中。

7。指令集

EVM的指令集在房间里保持在最低限度，以尽可能避免可能导致共识问题的错误。。所有指令都在256位的基本数据单元上操作。它们具有常见的算术、位、逻辑和比较操作，还可以进行有条件和无条件跳转。您可以访问当前的相关属性，例如它的编号和时间戳。

8。消息呼叫

合约可以通过消息调用的方式调用其他合约，或者发送以太币到非合约账户。消息调用和事务非常相似，它们都有一个源、一个目标、数据加载、以太坊、Gas和返回数据。。实际上，每一个事务都可以看作是一个顶级的消息调用，依次会产生更多的消息调用。

如果在内部消息调用期间发生气体用尽异常或其他异常，合同可以确定剩余气体的分配。合同会通知。被调用的契约将拥有全新的内存，可以访问被调用的负载。

9。代码调用和库

以太坊中有一种特殊类型的消息调用，叫做callcode。。它与消息调用几乎完全相同，只是从目标地址加载代码将在调用协定的上下文中运行，这意味着协定可以在运行时从另一个地址动态加载代码。存储、当前地址和余额都指向发起呼叫的合同。仅从被叫地址获得代码。这使得Solidity能够实现一个&quot图书馆&quot。可重用的库代码可以应用于合同的存储，并可以用于实现复杂的数据结构，从而使智能合同更加强大。