区块链 | 详解以太坊的工作原理

不管你们知不知道以太坊Ethereum blockchain是什么，但是你们大概都听说过以太坊。最近在新闻里出现过很多次，包括一些专业杂志的封面，但是如果你们对以太坊到底是什么没有一个基本的了解的话，看这些文章就会感觉跟看天书一样。 所以，什么是以太坊？本质上，就是一个保存数字交易永久记录的公共数据库。

作者：佚名 来源：Linux中国 | 2018-06-01 09:17

简介

Ethereum blockchain

不管你们知不知道以 太 坊是什么，但是你们大概都听说过以太坊。最近在新闻里出现过很多次，包括一些专业杂志的封面，但是如果你们对以太坊到底是什么没有一个基本的了解的话，看这些文章就会感觉跟看天书一样。 所以，什么是以太坊？本质上，就是一个保存数字交易永久记录的公共数据库。重要的是，这个数据库不需要任何中央权威机构来维持和保护它。相反的它以一个“无信任”的交易系统来运行——一个个体在不需要信任任何第三方或对方的情况下进行点对点交易的架构。

依然感到很困惑？这就是这篇文章存在的理由。我的目标是在技术层面来解释以太坊的工作原理，但是不会出现很复杂的数学问题或看起来很可怕的公式。即使你不是一个程序员，我希望你看完之后最起码对技术有个更好的认识。如果有些部分技术性太强不好理解，这是非常正常的，真的没有必要完全理解每一个小细节。我建议只要宏观的理解一下事物就行了。

这篇文章中的很多议点都是以太坊黄皮书中讨论过的概念的细分。我添加了我自己的解释和图表使理解以太坊更加简单一点。那些足够勇敢的人可以挑战一下技术，去阅读一下以太坊的黄皮书。

好了， 让我们开始吧！

猜您喜欢 换一换

企业引入物联网前必须考虑的5大挑战
郑伟 2天前

你应该了解的6个开源AI工具
Sam Dean 2天前

外媒速递：Linux小攻略¯关于history命令的...
核子可乐译 2天前

数据中心运维的二次革命
佚名 2天前

Python 之父宣布退出决策层，Python 该何去...
佚名 2天前

通过抓包，实现Python模拟登陆各网站，原理...
空手忆岁月 2天前

迁移数据中心时遇到的风险有哪些，如何应对？
佚名 2天前

机房存在哪些安全隐患？需要排查哪些地方？
数据中心运营管理 2天前

第四范式 / 智能推荐

编辑推荐

热点 80万年薪挖不来一个区块链工程师，转型潮却远未到来

头条 盘点国内十个最大以区块链为名义进行诈骗的项目

关注 区块链硅谷之争，中国已掉队？

头条 深度解析：区块链的数据存放在哪？如何保存个人的信息数据？

关注 华为云应用服务“完美搭配”助力企业开发上云更高效

24H热文 一周话题 本月最赞

物联网有望成为区块链的杀手级应用
区块链入门教程第一期：区块链
区块链入门教程第二期：挖矿？
3000多人被骗3亿元！又一区块链骗局曝光
看看区块链未来应用的36种场景，有你从事...

区块链定义

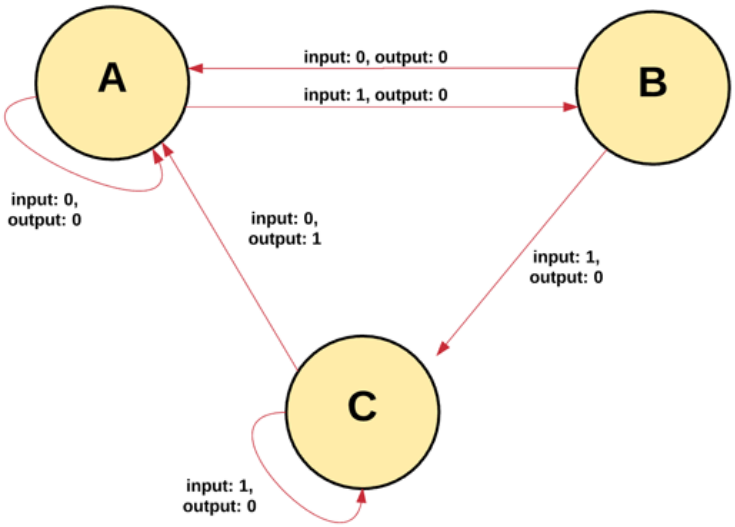
区块链就是一个具有共享状态的密码性安全交易的单机（cryptographically secure transactional singleton machine with shared-state）。这有点长，是吧？让我们将它分开来看：

> “密码性安全”（Cryptographically secure）是指用一个很难被解开的复杂数学机制算法来保证数字货币生产的安全性。将它想象成类似于防火墙的这种。它们使得欺骗系统近乎是一个不可能的事情（比如：构造一笔假的交易，消除一笔交易等等）。
>
> “交易的单机”（Transactional singleton machine）是指只有一个权威的机器实例为系统中产生的交易负责任。换句话说，只有一个全球真相是大家所相信的。
>
> “具有共享状态”（With shared-state）是指在这台机器上存储的状态是共享的，对每个人都是开放的。

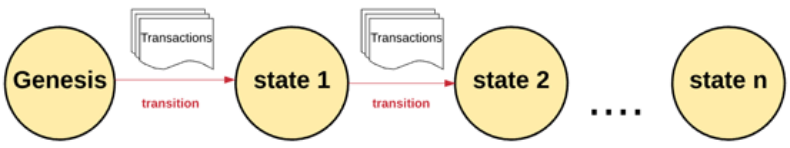
以太坊实现了区块链的这个范例。

以太坊模型说明

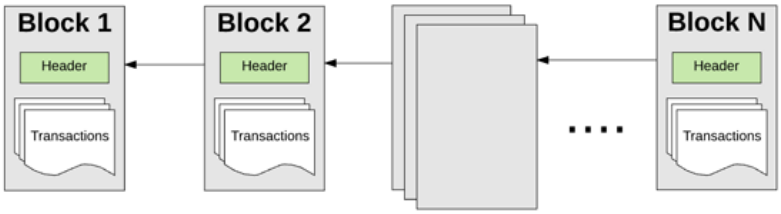
以太坊的本质就是一个基于交易的状态机（transaction-based state machine）。在计算机科学中，状态机 是指可以读取一系列的输入，然后根据这些输入，会转换成一个新的状态出来的东西。



根据以太坊的状态机，我们从创世纪状态（genesis state）开始。这差不多类似于一片空白的石板，在网络中还没有任何交易的产生状态。当交易被执行后，这个创世纪状态就会转变成最终状态。在任何时刻，这个最终状态都代表着以太坊当前的状态。



以太坊的状态有百万个交易。这些交易都被“组团”到一个区块中。一个区块包含了一系列的交易，每个区块都与它的前一个区块链接起来。



为了让一个状态转换成下一个状态，交易必须是有效的。**为了让一个交易被认为是有效的，它必须要经过一个验证过程，此过程也就是挖矿**。挖矿就是一组节点（即电脑）用它们的计算资源来创建一个包含有效交易的区块出来。

任何在网络上宣称自己是矿工的节点都可以尝试创建和验证区块。世界各地的很多矿工都在同一时间创建和验证区块。每个矿工在提交一个区块到区块链上的时候都会提供一个数学机制的“证明”，这个证明就像一个保证：如果这个证明存在，那么这个区块一定是有效的。

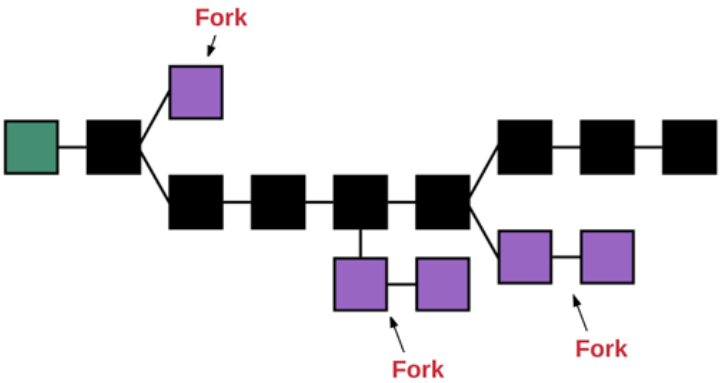
为了让一个区块添加到主链上，一个矿工必须要比其他矿工更快的提供出这个“证明”。通过矿工提供的一个数学机制的“证明”来证实每个区块的过程称之为工作量证明（proof of work）。

证实了一个新区块的矿工都会被奖励一定价值的奖赏。奖赏是什么？以太坊使用一种内在数字代币——以太币（Ether）作为奖赏。每次矿工证明了一个新区块，那么就会产生一个新的以太币并被奖励给矿工。

你也许会在想：什么能确保每个人都只在区块的同一条链上呢？我们怎么能确定不会存在一部分矿工创建一个他们自己的链呢？

前面，我们定义了区块链就是一个**具有共享状态的交易单机**。使用这个定义，我们可以知道正确的当前状态是一个全球真相，所有人都必须要接受它。拥有多个状态（或多个链）会摧毁这个系统，因为它在哪个是正确状态的问题上不可能得到统一结果。如果链分叉了，你有可能在一条链上拥有 10 个币，一条链上拥有 20 个币，另一条链上拥有 40 个币。在这种场景下，是没有办法确定哪个链才是最”有效的“。

不论什么时候只要多个路径产生了，一个”分叉“就会出现。我们通常都想避免分叉，因为它们会破坏系统，强制人们去选择哪条链是他们相信的链。



为了确定哪个路径才是最有效的以及防止多条链的产生，以太坊使用了一个叫做“GHOST 协议”（GHOST protocol）的数学机制。

手把手教你设计CPU——RISC-V处理器篇

CPU

精彩评论

sqskg评论了：高通华裔工程师跳楼自杀！中年IT男，为何这么难？

这里说的确实比较现实，也比较残酷；

白色面具评论了：“无限流量”套餐偷偷扣钱，工信部都看不下去了！

都是套路 国企和部门联合套路吃瓜群众

yeshou评论了：再见铁饭碗！又一个行业被颠覆！中国建设银行正式宣布

谁又在贩卖焦虑。

wx5b4431ad1fa56评论了：如何配置MySQL数据库超时设置

好文章

精选博文 论坛热帖 下载排行

- 动态路由之OSPF和RIP协议实现全网互
- 在华为RH2288HV3上部署RAID
- OSPF高级设置实现全网互通
- springboot + shiro 权限注解、统一
- windows共享文件分析

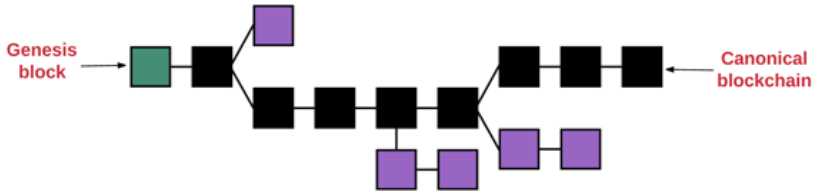
读 书 +更多

《网管员必读——网络管理》

本书在全面介绍微软最新网络操作系统Windows Server 2003的基础上，简要地介绍了UNIX和Linux两大操作系统的代表产品：Sun（太阳）公司的Sol...

GHOST = Greedy Heaviest Observed Subtree

简单来说，GHOST 协议就是让我们必须选择一个在其上完成计算最多的路径。一个方法确定路径就是使用最近一个区块（叶子区块）的区块号，区块号代表着当前路径上总的区块数（不包含创世纪区块）。区块号越大，路径就会越长，就说明越多的挖矿算力被消耗在此路径上以达到叶子区块。使用这种推理就可以允许我们赞同当前状态的权威版本。



现在你大概对区块链是什么有个理性的认识，让我们在再深入地了解一下以太坊系统主要组成部分：

accounts
账户
state
状态
gas and fees
损耗和费用
transactions
交 易
blocks
区块
transaction execution
交 易 执 行
mining
挖矿
proof of work
工作量证明

在开始之前需要注意的是：每当我说某某的哈希， 我指的都是 KECCAK-256 哈希，以太坊就是使用这个哈希算法。

【编辑推荐】

1. 区块链乱象丛生屡禁不止 多个难题亟待解决
2. 人工智能冰淇淋机亮相北京；IBM用“AI+区块链”鉴定钻石
3. 支付宝暖爸工程师手绘区块链童话故事 7岁儿子一个问题把他难住了
4. 区块链成香饽饽，加密货币却成落汤鸡
5. 关于物联网(IoT)，区块链可能会如何影响你我的生活？

【责任编辑：庞桂玉 TEL：（010）68476606】

点赞 0