

区块链入门教程第一期：区块链

区块链 (blockchain) 是眼下的大热门, 新闻媒体大量报道, 宣称它将创造未来。可是, 很多人都是为了炒币来的。对于区块链到底是什么, 有何特别之处根本不知道, 也没兴趣了解。那么区块链到底是什么呢?

作者: BCTOPIA区块链学院 来源: 今日头条 | 2018-06-14 11:02

收藏 分享

开发者盛宴来袭！7月28日51CTO首届开发者大赛决赛带来技术创新分享

区块链 (blockchain) 是眼下的大热门, 新闻媒体大量报道, 宣称它将创造未来。可是, 很多人都是为了炒币来的。对于区块链到底是什么, 有何特别之处根本不知道, 也没兴趣了解。那么区块链到底是什么呢?



一、区块链的本质

区块链的本质是什么? 一句话, 区块链本质上是一个去中心化的分布式账本数据库。

首先, 区块链的主要作用是储存信息。你可以将你需要保存的信息, 都可以写入区块链, 也可以从里面读取。

其次, 任何人都可以架设服务器, 加入区块链网络, 成为一个节点。一旦加入, 该节点享有同其他所有节点完全一样的权利与义务, 也就是说每一个节点都是平等的。你可以在任意的节点进行读写操作, 最后全世界所有节点会根据某种机制的完成一次又一次的同步, 从而实现在区块链网络中所有节点的数据完全一致。

猜您喜欢

换一换

专为公共云的Minimal Ubuntu发布: 体积减...
佚名 13小时前

如何在Arch Linux中查找已安装的专有软件包? ...
Sk 13小时前

大厂经验: 两步搞定PHP-FPM优化, 让服务器...
猛哥 1天前

迁移到Linux: 使用sudo
John Bonesio 7小时前

还有多少个X站在被后门、webshell寄生?
佚名 1天前

你可能不知道, iPhone 计算器原来这么好用
佚名 10小时前

PTC为工业企业提供清晰的AR价值路径, 热门...
佚名 11小时前

从私有云迁移到混合云并不容易
佚名 10小时前

编辑推荐

关注 区块链也不安全 三大攻击维度必须了解

头条 区块链难道仅仅只是“币圈大佬”割韭菜的工具?

热点 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?

头条 苹果进击区块链, 手机丢了随时可以找回来!

热点 区块链投资切勿盲目跟风“网红”的诱惑

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

区块链科普: 非对称加密、椭圆曲线加密算法

苹果进击区块链, 手机丢了随时可以找回来!

80万年薪挖不来一个区块链工程师, 转型潮...

区块链硅谷之争, 中国已掉队?

区块链也不安全 三大攻击维度必须了解



深度解析：区块链的数据存放在哪？如何保...
"区块链预测"搭上世界杯 "只赢不输"背后藏...

二、区块链的特点——去中心化

区块链最大的特点就是去中心化。想要了解去中心化，就先得知道什么是中心化。

什么是中心化呢？打个比方，就比如你在淘宝买东西，就算你付款了，资金不是去了卖家那里而是在支付宝那里，只有当你确认收货了，资金才会从支付宝转到卖家账户里面。也就是说，本来是买卖双方之间的交易，中间却多了个支付宝这个第三方，这就是中心化，支付宝就是那个中心。

这样，去中心化就很明显了，就是不需要第三方，买卖双方直接进行的交易。

区块链就是这样，区块链没有管理员，它是去中心化的。其他的数据库都有管理员，区块链没有。但是，没有了管理员，人人都可以往里面写入数据，怎样才能保证数据是可信的呢？被坏人改了怎么办？请接着往下读。


三、区块链的组成

区块链由一个个区块（block）组成。区块很像数据库的记录，每次写入数据，就是创建一个区块。每一个区块包含了两个内容：区块头和区块体。


区块头：记录这个区块的特征，包括时间戳、上一个区块的Hash（哈希）、区块体的Hash等等。

区块体：储存的信息，也就是实际数据。


视频课程 +更多



【吴刚】AE（After Effects）零基础入门标准
讲师：吴刚 112065人学习过



【吴刚】字体设计与表现视频教程
讲师：吴刚 151963人学习过



Python3数据处理Pandas快速入门视频课程
讲师：张敏 810人学习过

CTO专属活动 +更多

申请试听：CTO的4D领导力，打造你的管理

白熊视频：揭秘京东618背后的程序员GG

走访美团：美团背后的技术基因


CTO训练营

申请入营	互联网班	金融班
------	------	-----


CTO俱乐部

申请加入	最新活动	全部课程
------	------	------


最新专题 +更多



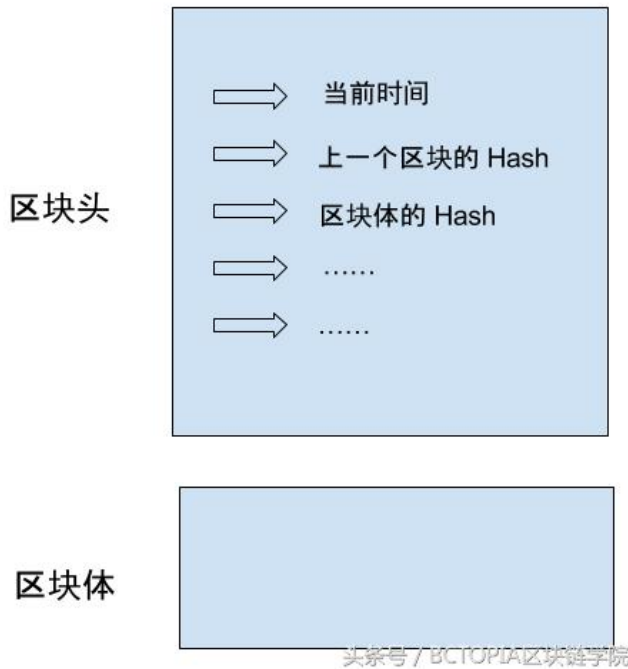
ThinkPad 三大商用解决方案
成就企业未来
ThinkPad



运维的下一幕思考：基于实际场景的AI Ops实践解析
运维/思考/AI Ops



精通数据科学：从线性回归到深度学习
数据科学



这里，就又有问题来了，什么又是哈希？

所谓"哈希"就是计算机可以对任意内容，计算出一个长度相同的特征值。区块链的 哈希长度是256位，这就是说，不管原始内容是什么，最后都会计算出一个256位的二进制数字。而且可以保证，只要原始内容不同，对应的哈希一定是不同的。

举例来说，字符串123的哈希是a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0（十六进制），转成二进制就是256位，而且只有123能得到这个哈希。（理论上，其他字符串也有可能得到这个哈希，但是概率极低，可以近似认为不可能发生。）。

也可以这么说，每一个区块的Hash都是不一样的，每一个Hash对应一个区块，如果区块发生改变，区块对应的Hash也将发生变化。

四、Hash 的不可修改性

区块与哈希是一一对应的，每个区块的哈希都是针对"区块头"（Head）计算的。也就是说，把区块头的各项特征值，按照顺序连接在一起，组成一个很长的字符串，再对这个字符串计算哈希。

Hash = SHA256（区块头）

上面就是区块哈希的计算公式，

SHA256是区块链的哈希算法。注意，这个公式里面只包含区块头，不包含区块体，也就是说，哈希由区块头唯一决定，

前面说过，区块头包含很多内容，其中有当前区块体的哈希，还有上一个区块的哈希。这意味着，如果当前区块体的内容变了，或者上一个区块的哈希变了，一定会引起当前区块的哈希改变。

这一点对区块链很重要。如果有人修改了一个区块，该区块的哈希就变了。为了让后面的区块还能连到它（因为下一个区块包含上一个区块的哈希），该人必须依次修改后面所有的区



Spring微服务实战

Spring

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；



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



wx5b447518e9d9c评论了：偶数科技构建新一代数据仓库，与AI应用场景更契合

人工智能在各行业的应用越来越广泛了，看好偶数科技

精选博文 论坛热帖 下载排行

部署Apache网站服务以及访问控制的实
Web必备性能压力测试工具WebBench与A
mysql的组复制
详谈iptables防火墙
centos7部署MongoDB数据库复制集（超

读书

+更多



Cisco网络工程案例精粹

《Cisco网络工程案例精粹》是一本以案例为基础兼顾知识概述的案例性书籍，所收录的案例都是笔者精心挑选出来的在网络工作中常见的案例。 ...



订阅51CTO邮刊

点击这里查看样刊

立即订阅

块，否则被改掉的区块就脱离区块链了。由于后面要提到的原因，哈希的计算很耗时，短时间内修改多个区块几乎不可能发生，除非有人掌握了全网51%以上的计算能力。

正是通过这种联动机制，区块链保证了自身的可靠性，数据一旦写入，就无法被篡改。这就像历史一样，发生了就是发生了，从此再无法改变。这样保证了安全性。



头条号 / 51CTOPIA区块链学院

五、总结

区块链作为无人管理的分布式数据库，从2009年开始已经运行到现在，没有出现大的问题。这证明它是可行的。

但是，为了保证数据的可靠性，区块链也有自己的代价。一是效率，数据写入区块链，最少要等待十分钟，所有节点都同步数据，则需要更多的时间；二是能耗，区块的生成需要矿工进行无数无意义的计算，这是非常耗费能源的。

因此，区块链的适用场景，到现在为止其实非常有限。

但区块链是互联网金融的底层技术架构。区块链在未来的发展，才能够带来互联网金融的发展。

所以让我们期待区块链给我们带来更智能、更实时、更普惠的未来金融！

第二篇文章《[区块链入门教程第二期：挖矿](#)》已发，感兴趣的朋友自行阅读！

【编辑推荐】

1. [2018年区块链高考统一试题（A、B卷）](#)
2. [说起来容易做起来难，区块链实施需要注意哪些？](#)
3. [3000多人被骗3亿元！又一区块链骗局曝光](#)
4. [区块链能够给物联网带来什么？](#)
5. [区块链原理是什么？如何开发区块链程序？](#)

【责任编辑：庞桂玉 TEL：（010）68476606】

点赞 1

51CTO区块链社群正式开通

全球视野下的行业大势、国内外最新政策、区块链技术应用、案例解析、数字货币市场动态、相关投资经验.....区块链领域全方位价值信息，尽在51CTO区块链社群。大势已来，让我们共同缔造历史！



51币读官微