区块链技术是从虚拟货币BTC中剥离的一门技术。区块链说白了是 区块+链，中本聪创立了比特币，换言也是区块链技术的创始人。这里为你解释何为区块链，挖矿到底在干什么？

前言

在比特币刚发行的时候人们发现了，它去中心化，不受任何中心管制；它完全开放，除了交易信息加密之外整个系统信息高度透明，技术都是开源的；安全性，只要不能控制全部节点的%51，就无法肆意修改数据，这使得它相对安全；独立性，整个模式和比特币不依赖任何第三方，所有节点都在系统内验证、交换数据，不受任何干预

我们这里详细解释什么是区块链技术，说白了就是区块+链，那什么是 “区块”？什么又是 “链” 呢？

区块 链

区块就是一个账本交易记账由分布在不同地方的多个节点共同完成，而且每一个节点记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证

每一个区块包含了前一个区块的加密散列、相应时间戳记以及交易资料（通常用默克尔树（Merkle tree）算法计算的散列值表示），这样的设计使得区块内容具有难以篡改的特性。用区块链技术所串接的分布式账本能让两方有效记录交易，且可永久查验此交易。

哈希函数

哈希函数h（ ）的作用：将任意长度的字符串，转换成固定长度（例如256位）的输出。输出也被称为哈希值，这个输出不可逆

很难找到两个不同的x和y，使得h（x） = h（y），也就是说两个不同的输入，会有不同的输出。理论上说两个不同的输入可能会有不同的输出，但这几乎不可能，比方说一个无限的空间映射到一个有限的空间，肯定存在多对一的情况，理论存在，但没有任何规律，保证你无法通过数学上的任何推断来找到这个结果，为什么这

里是256位呢？不是更长的呢？因为256位已经足够安全。

将账本拆分成块，比如一个本子的一张纸就是一个区块，每个区块记录一段时间内的交易，列如10分钟

我们把每张纸比作一个一个区块
，在每个区块的上面增加一部分
内容我们把它叫做区块头
，其中记录父区块的哈希值，通过每个区块储存父区块的哈希值，将所有区块按顺利连接起来，形成区块链

把1区块的哈希值记录到2区块
的区块头上，如此操作每个区块的区块头都记录父区块的哈希值，每个区块都按照顺序链接起来了，这就叫做区块链。第一个区块没有区块头，又被称之为创世区块

防篡改区块交易记录

- 形成区块后，篡改任一交易，会导致该交易区块哈希值和其子区块中不同，发现篡改
- 即使继续篡改子区块头中哈希值，会导致子区块哈希值与孙区块中不同，发现篡改
- 只要记录最后一个区块的哈希值，任何篡改都能发现

本质

- 一个人人可见的大账本，只记录交易
- 核心技术：通过密码学 + 数据结构，保证账本记录不可篡改
- 核心功能：创造信任。

区块链技术拓展

区块链是一个账本，在账本上只有发生了交易你的账户上的钱才会变多和变少，需要进行交易那么首先需要一个账号和密码，就像你的银行卡有账号和密码别人就可以对你进行一个转账，在区块账本上这个账号密码就是公钥和私钥

- 私钥：一串256位的二进制数字，私钥你甚至可以直接抛硬币决定，一般使用钱包软件帮助产生私钥，也是随机产生的。但是丢失了你的私钥之后你的账户、钱也随之丢失

- 公钥：私钥转化而成，但是地址无法反推私钥。在比特币中你的地址就是你的id，如果你想，你可以拥有n个id，只有产生交易进入区块链账本后才被大家知道
- 地址：公钥太长了，所以就有更短一些的地址的概念。地址通过摘要算法生成，通过地址不会暴露公钥内容

数字签名技术

老王（已有私钥，公钥），想转给张10个BTC，需要一些操作

证明是老王本人发出转账签名函数Sign（老王的私钥 +
转账信息：老王转给张三10 BTC）=本次专账签名
验证是老王本人发出转账验证函数Verify（老王的地址 +
转账详细：老王转给张三10 BTC + 本次转账签名）=true
一旦转账记录到区块从此谁也不能改变它，张三增加10 BTC，老王则相应减少10 BTC，整个操作都是自动的，比如你的钱包app它会帮你去做这样的事情，app知道你的私钥，你告诉钱包交易内容，钱包签名向全网公布，等待其他人来验证这笔交易

去中心化

中心化记账效率会更高，银行、政府或者支付宝帮你记账，都很可靠，因为他们都无法动你的钱，除非它们有你的私钥

中心化记账存在一些缺点

- 中心机构拒绝或停止服务
- 中心机构容易遭受攻击（服务器被攻击、政府干预、法律终止、自盗等）
- 中心机构资源有限
- 信任往往被辜负，如某人利用漏洞在银行增加自己的财富
- 避免自己的财富被稀释，中心机构超发货币

去中心化人人都可以记账，每个人可以保留一个完整的账本。任何人都可以下载开源程序，参与比特币的p2p网络，监听来自全世界发送的交易，成为记账节点，参与记账，假设小逸发布了一笔交易向全网广播，A记账节点监听到了这笔交易，A验证了这笔交易位true之后放入交易池继续向其它节点传播，因为是网络传播，同一时间不同记账节点的交易池不一定相同，每10分钟，从所有记账节点当中，按照某个方式抽取一名，验证这个节点的交易为true之后，之后将这个选中的节点交易池

中的交易记录与自己（A）节点的交易池中的交易记录对比一下，对比完之后会将自己交易池中已经被选中记账节点记录的交易删掉，别的不动继续记账等待下一次被选中，每隔10分钟就是一个循环，这个10分钟所有记账节点正常记账，10分钟之后再选出一个节点把它交易池当中的交易作为一个新的区块，这个区块来自所有记账节点中我任意选择的一个记账节点的交易池，如此不断循环往复

交易并不是被记录就完成，只有当这笔交易变成了某一个区块，这笔交易才算是真正的完成。这就是去中心化的一个记账的完整的流程，你的交易并不会第一时间被记录，因为p2p网络传播需要时间，如果被选中区块的节点还没有接受到你的交易，交易就没有完成。每10分钟产生一个区块，但不是所有在10分钟内的交易都能记录。10分钟只是一个平均值

去中心化记账的特点，有记账权的记账节点，每十分钟被选中的节点它会获得50BTC奖励，每21万个区块差不多4年，奖励减半，比特币自发行已经两次减半，那么每十分钟产生一个新的区块这个记账节点得到的奖励是10.5BTC，每隔4年减半那么可以算出BTC的总量大约为2100万枚，预计2040年开采完，记录一个区块的奖励也是比特币唯一的发行方式，当BTC开采完之后，记账节点可以获得的收益就只有交易的手续费了

记账权分配

记账节点通过题目来争夺记账权，

找到某位随机数使得等式不成立
SHA256哈希函数（随机数 + 父区块哈希值 + 交易池中的交易）> 某一指定值）
从0开始遍历
随机数碰运气之外，没有
其它解法，解题的过程，又叫做挖矿
，所以解这个题目的记账节点又被称之为矿工
，你遍历随机数越快你拿到这个记账权的可能性就越大，这个遍历速度就被矿老板们称之为算力，为了得到这个算力，矿老板们就会购买更多且更高算力的矿机

谁先解对，谁就得到记账权。A记账节点率先找到解，即向全网公布，其他节点验证无误之后，A节点就获得了这个区块，获得12.5个BTC的收益，在新区块之后重新开始新一轮计算。这个方式被称之为（POW）分配记账权

一般大约10分钟解出这个随机数，10并不绝对，因为解开这个题目的过程本就是个碰运气的过程，未来应对算力的变化，比特币每隔2016个区块，大约两周，会加大或减小难度，使得平均产生区块的时间是十分钟

总结

每一个区块包含了前一个区块的加密散列、相应时间戳记以及交易资料（通常用默克尔树（Merkle tree）算法计算的散列值表示），这样的设计使得区块内容具有难以篡改的特性。用区块链技术所串接的分布式账本能让两方有效记录交易，且可永久查验此交易。

和传统存储的数据不同的是，区块链每个节点都按照块链式结构存储完整的数据，区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。

一句话解释区块链

麻将作为中国传统的区块链项目，四个矿工一组，先碰撞出13个数字正确哈希值的矿工可以获得记账权并得到奖励。

题外话

很多人讲区块链是骗局比特币是骗局，这也许是个骗局，但是这个技术已经被广泛地承认和应用，区块链涉及的密码学知识一般人再借几个脑子给你你也搞不懂，在一个相对理性的角度看待问题最重要，千万别听风就是雨。

这门技术有着不可思议的地方
在一个没有中心没有监管的情
况下保持着绝对的秩序
这个只需由大家的共识建立的信任，比特币创造了这个共识，在区块链的世界里每个人都是公平平等的。