图片源自百度下载

区块链是什么，有点类似一串珍珠项链，其中每颗珍珠都有固定的位置，拿走任何一颗珍珠，其他珍珠的位置都会发生变化。每颗珍珠就相当于一个区块，将珍珠用线串起来就形成了区块链。当然这样的比喻不是非常贴切，只是为了方便大家理解。

第一个区块链应用——比特币，它的工作原理类似打麻将，4个矿工自发地组织在一起，通过掷骰子（碰撞一个随机数）确定谁来记账，谁获得了记账权谁就得到了相应的奖励，其他3个矿工对这笔账目进行确认。这个账本与我们之前使用的账本不同，由于它是一群人来记账，因此修改这个账本的难度会比较高。

我们传统的信息系统，无论是银行系统，还是我们熟悉的支付宝、微信，使用的数据库都是集中式、中心化的，所有的数据安全都依赖于某一个组织（例如阿里）的可信度，以及这个组织背后的技术是否过硬，管理是否足够严格。

而区块链则不同，它是通过共识机制发动大量的节点来共同记账，并且这些节点之间地位平等。由于区块链采用了一群人共同记账的方式，使得数据难以篡改。

在区块链技术中，要修改数据必须得到半数以上节点的同意才可以修改数据，相对

于传统中心化单个节点说了算的记账方式，使用区块链技术进行记账可以提高大家的信任度，而这种信任机制的建立不依赖于某个组织、个人，而是依赖于区块链技术本身。

举一个例子，在一个村子里，张三借给李四1万元人民币，原来的方式就是张三给李四打一张借条，或者找一个双方都信得过的人作为见证人。现在有了区块链，同样是张三借给李四1万元人民币，我们会发动所有的人都来记账，每个人都会在自己的本子上记一笔账“张三借给李四1万元人民币”。按传统的记账方式，一旦李四的借条丢了，或者张三贿赂了这位见证人，这笔借款都有可能收不回来。但有了区块链，由于全村人都记账，这笔借款就变得无法抵赖了。

那么，问题来了，凭什么全村人都帮李四来记这一笔账，只是人缘好是不能让全村人都来记账的，我们必须有一套机制来奖励这些人。这就有点像农村的红白喜事，全村人都来帮忙，原因是以前大家生活条件都不好，只要村中有红白喜事，当事人都要大摆宴席答谢村里人，这其实就是一种奖励机制。

同样，区块链要让一群不相干的人来共同记账，因此需要一套奖励机制，也就是经济刺激，让参与记账的人可以获得经济上的回报。但问题是，只要有经济刺激，就会有人作弊。

为了防止有人作弊，区块链引入了共识机制，以确保参与者无法作弊。比特币和现在的以太坊使用的共识机制是工作量证明机制（Proof of Work，PoW）；Bitshares、Steem、EOS采用的是代理权益证明机制（Delegate Proof of Stake，DPoS）。

为防止共识信息被篡改，典型的区块链会采用链状数据结构进行数据存储。因此，区块链也是一个“历史记录不可篡改的数据库”。传统数据库可以增、删、改、查（CURD），而区块链只能增加和查询，不能修改、不能删除。去中心化是区块链最重要的特征，指的是区块链在不依赖中心化组织的条件下，参与方（节点）可以通过共识机制达成一致，使区块链天然具备信任的基础。账务公开是区块链技术中一个常用方法，为了使参与方都可以记账和验证，通常情况下会将账务公开广播给全网。

可追溯特性是基于密码学的区块链链状数据结构保证的。为了确保交易的唯一性，有效防止双重攻击，使用时间戳技术为每一笔交易加盖时间戳。

区块链只能发币吗？

作为一个分布式账本技术，除了加密货币本身的应用之外，智能合约是区块链现在

一个主要的发展方向。全世界的精英都将重心放在了智能合约的大规模应用上。

那么，有没有一种更有效的办法来确保合同的执行呢？答案是将上面的合同内容写在智能合约中，一旦智能合约中某个条件达成，合约就会自动执行。由于区块链信任的特点，使合约的执行不依赖于任何现有的中心化机构，这样就可以有效解决传统合同出现纠纷的问题。

无论是显式的合同，还是日常生活中的各种交易都是一种契约关系。传统契约需要签字、盖章才具备法律效应。你可以将智能合约想象为一个自动售货机，使用智能合约就是不依赖人和现有中心化机构，合约可以根据预设的条件自动执行。

去中心化作为区块链一个重要的特点，指的是区块链在不依赖中心化组织的条件下，参与方可以通过共识机制达成一致，使区块链天然具备信任的基础。去中心化的英文是decentralized，原意如下：

将权力从中央转移到地方政府：

将大型组织部门的管理权，从单一集中管理转移到其他部门，通常情况下给予它们一定程度的自主权。判断一条链是否去中心化，可以以节点数量、节点的容错性和有多少人（组织）能够控制系统来衡量。

节点数量越多，系统可以容忍崩溃的节点越多；参与节点的人（组织）越分散，就代表一条链的去中心化程度越高，反之，一条链就趋向于中心化。

区块链作为一个分布式账本技术，可以应用在很多地方，但在具体业务上，需要和云计算、大数据、人工智能、物联网等技术结合起来才能满足实际业务需求。

例如，在商品溯源中，区块链可以从商品源头信息采集、原料来源追溯、生产过程、加工环节、仓储信息、检验批次、物流周转到第三方质检、海关出入境、防伪验证的全过程进行追溯；将商品信息采用分布式结构存储在各个节点上，使数据受多方监管，保证链上商品信息记录过程的真实性。区块链数据不可篡改的特点，可以有效保证上链商品信息无法篡改，使商品溯源的可信程度大幅度提升，但要避免源头造假，还需要借助物联网技术进行数据采集。

共识机制：

不只是区块链的特权，在人类历史发展的长河中，已经产生了许多的共识机制，例如国家、宗教、道德、科学等。我们对于一件事情好坏的判断，都基于各自的生活环境和认知水平，这也能很好地说明为什么价值观相同的人容易达成共识，同一个

地域的人容易达成共识。为了能够清楚地理解共识机制，我们需要搞清楚共识机制中的区块、生产者、验证者3个核心概念。以篮球比赛为例，在篮球比赛中比赛成绩就是区块，运动员是区块的生产者，裁判员是区块链的验证者。如果裁判徇私舞弊就会产生信任危机，无法保证比赛成绩的真实性，因此共识机制的关键就是保证区块生产和验证的安全。

工作量证明机制（Proof of Work，PoW）

全网通过竞猜随机数获取生产区块的资格，一旦某个节点作恶就会白白损失算力，无法成为合格的区块生产者，也无法获得奖励。工作量证明机制并非完美，其中被指责最多的主要有两点，一是浪费能源，二是风险和收益博弈必然导致联合挖矿，而大算力矿池可能会对系统的去中心化构成威胁。比特币采用的是工作量证明机制。由于比特币长期缓慢的发展，导致65%的算力已经被5个矿池所占有。理论上上讲，5大矿池联手可以对比特币网络发起51%的攻击。

权益证明机制（Proof of Stake，PoS）

节点被称为验证者，没有挖矿，节点通过验证交易则获取交易手续费，验证错误则没收押金。每次系统会根据抵押代币数量来随机选择验证者，抵押代币越多则被选为验证者的概率越大。举一个例子，如果A节点抵押了100个代币，B节点抵押了10个代币，那么A节点相对B节点就有10倍的验证机会。

P2P（peer to peer）

首先要澄清的是，网络是一种分布式应用架构，不是大家认为的P2P网络借贷，中文称为对等网络（也称点对点网络）。举一个例子，你通过微信给朋友老王发了一句话“在吗？”，这时老王会在自己的手机上看到这条信息。你以为这条消息是直接发给了老王，其实背后的流程是：你先将这条信息发给了微信服务器，然后微信服务器再将这条消息发给老王。在你完全不知情的情况下，有一个中间人在参与你们的交流，这个人就是微信服务器，它在帮你转发那条消息。节假日，如果微信服务器繁忙，它有可能会罢工，这时候可能这条消息就一直无法发送。但是，如果采用P2P网络，你和老王之间就可以直接通信了。由于在P2P网络中不存在特殊节点，因此，其他任何节点出现问题都不会影响你和老王之间的通信。

我相信大家对区块链已经有了很好的认识，接下去章节我们再来说说区块链背后深层次的理解，请大家拭目以待！

1. 随着国家和地方政策的纷纷出台，作为价值互联网，区块链的商业价值是什么？

2. 区块链会在哪些领域率先出现？
3. 哪些行业会被区块链颠覆？
4. 哪些领域背后正在暗流涌动？

都是相当有意思的话题，非常值得期待！