很多人认识区块链的入门通道、区块链应用鼻祖——比特币网络，相信很多小伙伴对它都不陌生。但你真的了解比特币网络背后的工作原理吗？比特币系统不属于任何一个人或任何一家公司 / 组织，也没有员工、老板和股东来维持它的运转。换言之，比特币系统不受任何人的控制。那全世界这么多的节点和参与者凭什么信任它呢？又如何避免比特币被非法复制呢？

本次万向区块链小课堂将系统性地介绍比特币的工作原理，以及比特币的底层技术——区块链在数字货币以外的商业应用潜力，保证「说人话」、言简意赅、通俗易懂，诚邀大家细品~

缺少银行这类管理中心的交易系统通常会面临以下 3 大挑战：

资产确权防止交易信息造假确定交易记录的可靠性和权威性

然而比特币在没有金融机构这样的第三方管理中介下，却能应对这三大挑战。看懂比特币如何应对这 3 大挑战，自然就能理解比特币的工作原理了。下面我们就来详细看看比特币是如何攻克这 3 大难关的。

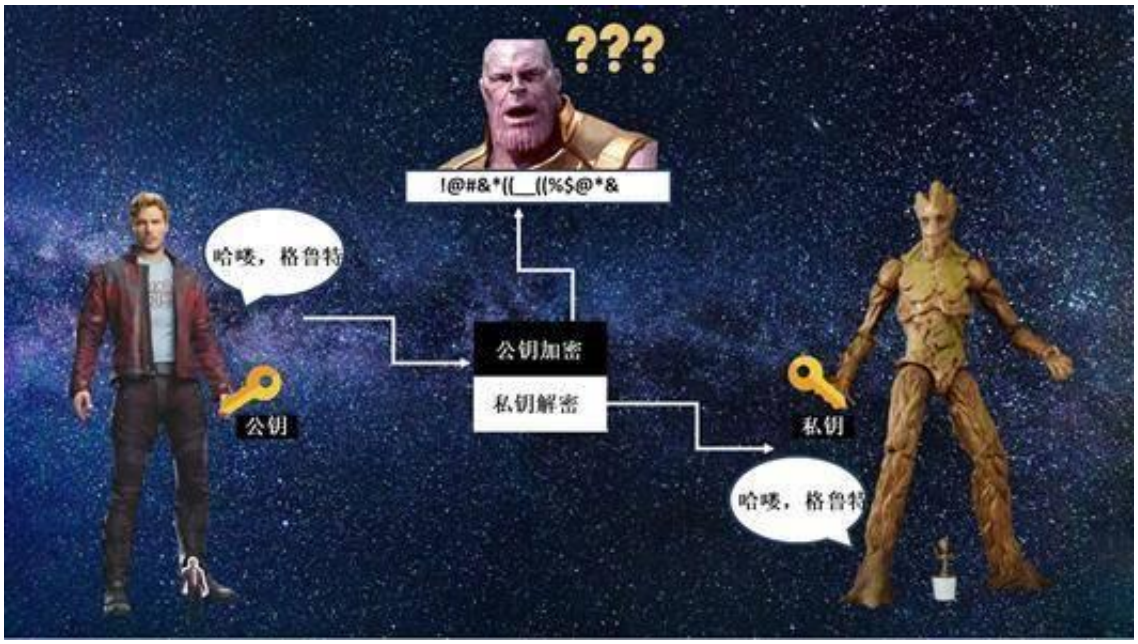
挑战一：资产确权

当有人向比特币区块链公布一笔交易记录时，如何确定这笔交易确实是由比特币的所有者发起的而不是骗子在意图造假呢？这就要用到计算机加密技术。

非对称加密

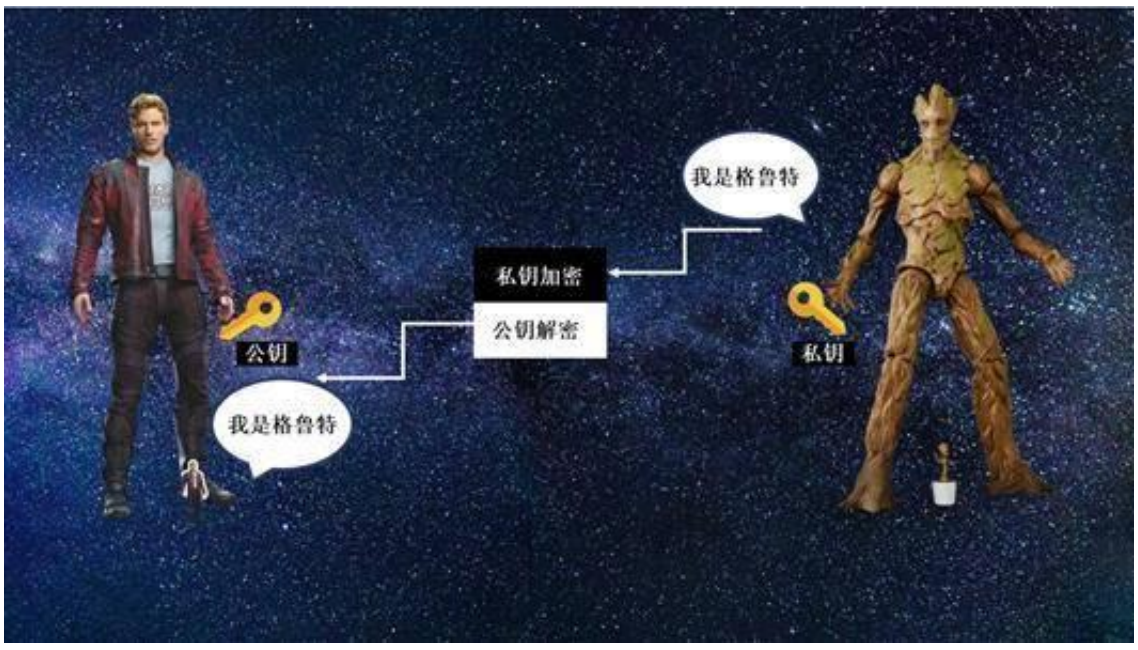
比特币采用的是非对称加密技术，需要用到一对密钥。经过其中一个密钥加密的数据可以用另一个密钥解密。使用过程中，公开一个密钥，即公钥，另一个非公开的密钥就对应地成为私钥（公钥类似互联网里的账号，私钥类似登陆密码）。

如何用这对密钥来发送信息呢？假设《银河护卫队》里的星爵想给格鲁特发送一条消息说：「哈喽，格鲁特」，但又要确保超级大反派灭霸不能读取这条消息，该怎么办呢？我们可以让格鲁特创建一对密钥，把公钥交给星爵，自己保管私钥。星爵可以用公钥加密信息，经过加密的信息看上去就像在胡言乱语，只有格鲁特用私钥解密之后才能知道星爵到底说了什么。



数字签名

比特币还会反向运用这对密钥来验证数据创建者的身份，即把密钥看作用户的数字签名。我们还是请银河护卫队来帮演绎这个情景。假设格鲁特想向星爵发送一条消息说「我是格鲁特」，但星爵如何确定这条信息真的来自格鲁特，而不是其他人冒充格鲁特发的呢？格鲁特可以用私钥加密这条信息，星爵收到信息后用对应的公钥解密信息，就可以读取「我是格鲁特」这条信息了。而且由于公私密钥的对应关系存在唯一性，星爵用公钥成功解密信息就能证明信息确实是由私钥持有者格鲁特发出的，否则星爵是不可能解开这条信息的。



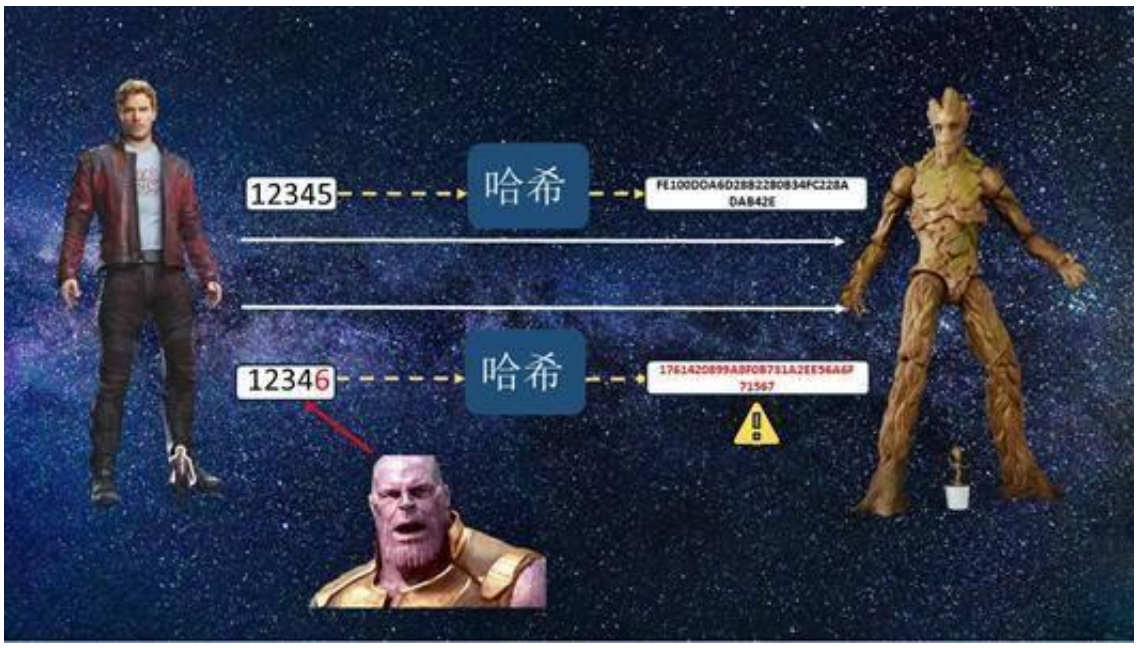
挑战二：防止交易信息造假

如果有人一个月前进行了一笔比特币交易，现在又反悔了，想悄悄撤回交易，比特币这一去中心化系统里又缺少权威的管理者，怎么才能让这种信息造假的阴谋无法得逞呢？这就要用到哈希算法。

哈希算法

哈希算法可以用于验证数据的真实完整性。任何信息可以通过哈希函数运算得到一个哈希值，但是原始信息发生丝毫改变都会让得到的哈希值变得完全不一样。

假设星爵想将「12345」这串数字传给格鲁特，又担心被灭霸中途截获，篡改信息。他可以算出这串数字哈希值：FE100DDA6D28B2280B34FC228ADAB42E，然后将这串数字和他的哈希值同时传给格鲁特。格鲁特在得到这串数字后同样进行哈希运算，看看得到的哈希值跟星爵告诉他的是否一致。如果一致，说明格鲁特和星爵拥有的原数字是一样的，这串数字在传输过程中没有遭到篡改或发生损坏。如果灭霸悄悄干预了数字传输过程，把原数字串改成了「12346」，再把错误数字传给格鲁特，格鲁特算出的哈希值就会是：1761420899A8F0B731A2EE56A6F71567，与星爵给他的截然不同，自然就会发现数据被篡改了。



区块链环环相扣

比特币中，固定时间段内的交易会被打包成一个区块。每个区块里都储存着前一个区块的哈希值。这些区块通过哈希值前后相连，形成链条状结构，也就是常说的区

块链。

下图中 3 个区块记录了交易 1 到交易 9 的信息。

如果删除掉第一个区块中的交易 3，那第 2
个区块中的哈希值就会发生变化，证明第 1 个区块中的交易信息被篡改了。

那可不可以尝试修改第 2 个区块，让它储存的哈希值呼应被篡改后的第 1
个区块中的信息呢？这也行不通。因为修改第 2 个区块中的信息后，第 3
个区块中的哈希值又无法与第 2 个区块的信息对应了，让人一眼就能知道第 2
个区块被篡改了。

由此可见，区块链上的信息是不可篡改的。随便改动一个区块中的信息，就会使其与后一个区块中的哈希值产生矛盾。只有逐个修改之后每个区块中的信息才能掩护最初这个信息篡改动作，这样一来原区块链的信息就会被彻底改变，相当于产生了一条新链。

挑战三：确定交易记录的可靠性和权威性

假设真有人篡改了每个区块中的信息，创建了一条新链，我们应该选择相信新链还是旧链呢？如何才能确定两者的可靠性和权威性呢？

工作量证明（Proof of Work）

这就要用到工作量证明。电脑会将前面讲过的哈希值转换成一串由「0」和「1」构成的数字：

00101110111101000000010000011010100100100010111011111000010010
10

我们可以规定只有哈希值以 0 开头的区块才能上链，这样就有 50%
的概率得到一个符合要求的区块。

0XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXX

同理，我们若规定只有哈希值以「00」开头的区块才能上链，概率就是 25%。

00XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXX

如规定哈希值必须以 32 个「0」开头的区块才能上链，那概率大概就只有 40 亿分之一了。

00000000000000000000000000000000XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

比特币区块链也设置了这样的规定。但是链上每个区块的哈希值都是恒定不变的，如何确保在输入固定信息的情况下能得到一个符合规定的哈希值呢？这就需要在每个区块中随机加入任意一个数值，也称为「随机数」（nonce）。

进行哈希运算的时候要将随机数与区块中的数据相结合。比特币区块链中遍布全世界的计算机要从大量的随机数中找到那个与现有区块结合后能算出以特定数量「0」开头的哈希值的随机数，才能让这个区块上链。这个寻找随机数的过程就是工作量证明。

这个过程会消耗大量算力，完成时间也难以估量。在比特币区块链中，平均 10 分钟会产生一个新区块。但由于该区块链中的整体算力水平一直在不断提高，为了增加找到随机数的难度，比特币区块链也在不断增加规定哈希值开头部分「0」的个数。

最长链原则

工作量证明这一规则有效限制了新区块产生的速率，那区块数量越多、长度越长的链存在的时间也就越久。因此，个人是不可能制造比官方比特币区块链更长的链的，除非这个人拥有的算力超过该系统中其他所有人算力的总和。

基于以上原因，当系统中出现多条链时，比特币用户只认可区块数量最多，存在时间最长的这条链，并相信这条链上的信息是权威可靠的。

区块链潜在的应用场景

除了比特币，区块链还有哪些应用前景？

我们在上文中从 3 方面简要解释了比特币区块链的工作原理：

用数字签名确权比特币用哈希验证链上交易的真实完整性用工作量证明避免虚假区块上链

由此可见，比特币就是一个人人都可以信任的去中心化账本。但是这个账本除了记录货币交易信息之外，还可以记录其他多种信息，让其他机构也能实现去中心化的信息分享。目前已在以下领域获得应用。

防止产品造假：生产商可以给每件产品贴上二维码，并把二维码编号记录到区块链中，该区块链就可以记录产品的流通信息，帮助消费者追踪产品是否来自可靠的生产商，是否是真品。目前药品生产行业造假情况日益严峻，危及病人健康，亟需这样的区块链解决方案。

防止物流信息造假：许多供应链庞大复杂的公司同样面临信息造假的困扰。他们可以通过打造私有链来追踪供应商的物流信息。私有链所有者有权决定区块链的参与方，供应链中的中心企业可以在私有链中给各个供应商设置不同权限。对于货物从小型供应商流转到中型供应商再流转到大型供应商最终进入生产商手中的多层级供应链来说，区块链有助于优化整个流程的管理。在这种多层级供应链中，小型供应商端稍有差错就会给生产商造成损失，但区块链技术可以使整个流程中的信息变得公开透明，方便所有参与方及时发现问题解决问题。万向区块链的供应链金融服务平台就是一个典型的应用案例。

促进协同合作：汽车保险理赔通常需要多家保险公司共享数据、协作解决。运用区块链管理相关信息和数据可以让这些保险公司放心地信任链上数据和信息的真实性，不需要再耗费人力检查验证数据和信息，从而为保险公司降低人力成本，同时提高理赔办理效率，提升车主满意度。

区块链商业挑战和机遇

近年来，区块链的概念被炒得很热，其中有很多夸大的成分。对于企业来说最关键的是要考虑是否有能力用好区块链。

另外，谁来为投资区块链买单也是一个问题。企业肯定会有这样的顾虑：凭什么要我花钱来打造一个区块链，方便行业里其他公司合作共赢？花钱的是我，结果好处却被大家瓜分了。这就体现了私有链和联盟链的优势，花钱打造私有链或联盟链的一方有权管理这个区块链，确保自身收益最大化。

尽管困难重重，但区块链蕴含的商业价值还是十分可观的。区块链的特性就是让互不信任甚至互为竞争对手的人或是企业能够放心地交换信息。所以要找到商业中信息交换不畅引发的问题，对症下药，运用区块链加以解决，就能让参与方各取所需，实现多方利益的最大化。