比特币原理通俗读本（比特币百喻经）

作者：比特百晓生

比特币是第一种去中心化的互联网货币，诞生于 2009 年初。英文名称“Bitcoin”，缩写及货币代码“BTC”。

【密蜂】中心化社会可以比喻为蜜蜂族群。蜂王是蜂群的中心，吃得最好，安逸悠闲，寿命 4－6 年。工蜂在蜂群中数量最多，但吃得最差，做的是苦工，寿命只有 2 个月。中心化社会也是脆弱的，“擒贼先擒王”，如果蜂王死了，整个蜂群就会灭绝。

特性：因为去中心化，所以比特币没有央行式的发行机构，没有银行式的管理机构，技术规则不能被任何机构强行更改，很难被封杀。它的货币总量是有限的，上限是 2100 万个，约在 2140 年到达。截止到 2014 年 4 月 6 日，已发行 1260 万个。它不能被冻结，可以自由跨国转帐，没有任何额度限制。系统每天 24 小时不间断运行，到帐速度很快。手续费很低廉，远低于国际汇款。如果用户认为有必要，还可以做到半匿名。

比特币没有实物，它在互联网里去中心化的 P2P 网络（对等网络，或称点对点网络）中运行，以“区块链”的形式，保存在公开的分布式数据库中，任何人都可以下载。

【帐本、复印】：区块链可以比喻为一个公开的帐本，下载区块链可以比喻为复印这个帐本，任何人都可以复印。

区块链是由一个一个的“区块”串联起来，象一根链条，有始无终。不断延长。平均每十分钟产生一个新区块，添加到区块链的尾部。

【帐单】：一个区块可以比喻为一页帐单，从下到上叠起来成为一个帐本。新的帐单添加到帐本的最上面，不断的增厚。

推算余额：每个区块包含了十分钟内发生的所有转帐交易。比特币不记录每个帐户的余额，只记录交易，然后根据交易推算每个帐户的余额。例如你有两笔交易，第一笔收到 50 个比特币，第二笔支出 20 个比特币，那么你现在的余额就是 30 个比特币。

比特币的每笔交易，都由付款人用私钥签名，证明确实是他同意向某人付款，其它人无法伪造。

【指纹】：私钥签名可以比喻为按指纹，每个人的指纹都不相同，其它人无法伪造。

规则规定，把前一个区块整体算出一个散列值，记录在本区块里。它能表示各个区块的先后次序，并使以住的区块很难被非法修改。如果修改替换某个区块，则依据它算出来的散列值就会不同，又必须修改下一个区块……最终必须把它后面的所有区块都改一遍，这太难了。

【缩略图】：前一个区块的散列值可以比喻为缩略图。把前一页帐单拍照，缩小打印在本帐单的左上角，就是缩略图。它能表示各页帐单的先后次序，并使以住的帐单很难被非法修改。如果修改替换某页帐单，则它的缩略图就不同了，又必须修改下一页帐单……最终必须把它后面的所有帐单都改一遍，这太难了。

每个运行比特币客户端软件的人都可以制造区块。每个区块必需包含一个符合一定要求

的随机数，用 SHA－256 散列算法随机碰撞得到，需要很大的计算量。这称为“工作量证明”机制（POW），以此证明参与制造区块的人有诚意，愿意付出一定的成本，产生最快的那个新区块被大家承认。

【记帐、赛车、运动量证明】：制造区块可以比喻为做帐单，即记帐，每个人可以参与。随机碰撞计算可以比喻为赛车，需要很大的车动力。“工作量证明”可以比喻为“运动量证明”，最快跑完规定里程的人所做的帐单被大家承认（假设每台车都有办公电脑，做帐单是高度自动化办公，赛车才耗时间。到达终点后，轻敲一键，帐单就打印出来了，花费的时间可以忽略不计）。

随机碰撞使得算力最大的人不能每次都最快完成。但是根据概率，长期来说算力更大的人能拿到更多次数的区块制造权。

【抽签】：随机碰撞可以比喻为抽签。赛车时每个人的规定里程并不相同，每次抽签，有 5 公里、10 公里、15 公里。所以有运气的因素，跑得最快的人不一定每次都能最快跑完抽签的里程，但是长期来讲大家运气均等，跑得更快的人能拿到更多次数的记帐权。

为了争夺区块制造权，人们最初用 CPU，后来发现用显卡更有效率，再后来发明了更先进的 ASIC（专用集成电路），并且持续的改进它。这种现象被称为“算力军备竞赛”，使得系统算力持续飙升，早已超过全球最快的 500 台超级电脑算力之和。系统更强大更安全，但是成本也在同步飙升。

【职业赛车】：CPU 可以比喻为自行车，显卡可以比喻为摩托车，ASIC 可以比喻为汽车，“算力军备竞赛”可以比喻为“职业赛车”，综合实力超过 F1。但是专业车辆比较贵，持续不断的改进升级，成本飙升。

为了吸引更多的算力参与区块制造，系统在每个区块产生 50 个新的比特币付给区块制造者，这便是比特币发行。比特币的发行采用每四年减半的机制，在头四年产生总量的 50%，第二个四年产生总量的 25%……现在已经减半，每块产出新币只有 25 个。

【印钞】：比特币发行可以比喻为印钞，都是新货币流入社会。

有了钱，就有人专职做区块制造，包括一些并不热爱比特币的人。这类于挖金矿，他们自称为矿工。

【赛车手】：矿工可以比喻为职业赛车手，包括一些并不热爱比特币的人。

矿工越来越多，一个矿工挖到一个块需要很长时间，收入不稳定。于是出现了若干矿池，矿工们把自己的算力加入到矿池中联合挖矿。矿池挖到区块，扣除矿池管理成本后，把收益按贡献的算力比例分配给矿工。

【车队】：矿池可以比喻为车队。赛车手越来越多，一个赛车手拿到一次记帐权需要很长时间，收入不稳定。赛车手们带着自己的车加盟到车队中联合赛车。车队任何人做出一页帐单，扣除车队管理成本后，把收益按贡献的车辆性能比例分配给所有的加盟赛车手。

原来十分钟左右产生一个块，因为矿机计算速度越来越快，如果挖矿难度不变，出块时间将会越来越短。但系统会自动调整挖矿难度，如果全网算力变大，难度将上升，反之则下降，使得出块时间稳定在十分钟左右。

【改签】：挖矿难度调整可以比喻为改签。因为车速越来越快，如果抽签的里程不变，出帐单的时间将会越来越短。但规则会改签，如果车速整体升高，里程将加大（例如车速整体

提升十倍，则抽签平均里程也加大十倍，改抽 50 公里、100 公里、150 公里），反之则缩短，使得出帐单的时间稳定在十分钟左右。

转帐手续费：为了抑制无聊的转帐交易，也为了奖励矿工，比特币的转帐收取微量的手续费，目前一般每笔为 0.00001 个币。

每个矿工所在的位置不同，各自的网络传输速度也不同，可能不同的人最先接收到不同的新区块。例如一部分人先收到张三做的新区块，另一部分先收到李四所做的新区块，李三与李四都自称是最快完成的，那么哪一个有效呢？规则规定，暂时都有效，矿工们在他最先收到的新区块后面接着做下一个区块。这样就产生了链分叉，有两条分支链。直到有一条链更长，短链上的矿工就会放弃，转到长链上接着做。通常分叉不多见，分叉时间较短，废弃链也不会太长。

【分道赛车】：链分叉可以比喻为分道赛车。赛车没有裁判，因为每个赛车手的位置、角度不同，复印的速度也不同，可能一部分人先复印到张三做的新帐单，另一部分先复印到李四所做的，张三与李四都自称是最快跑完的，那么谁的新帐单算有效呢？规则规定，暂时都有效，赛车手在他最先复印到的帐单后面接着后面接着做下一页帐单。这样就分开成两个跑道赛车，直到有一个跑道做的帐单页数更多，少页跑道的赛车手就会放弃，转到多页的跑道上接着赛车。通常分道赛车不多见，时间较短，废弃的帐单页数也不会太多。

交易合法性检查：制造每个区块的矿工，会用客户端软件对每一笔交易做交易合法性检查，假冒他人签名付款（假冒指纹盗窃）、用不存在的比特币付款（用假炒）、付款余额不足等非法交易很容易被发现并拒绝，不会加入到新区块中。如果矿工协同作弊，也会被其它矿工与用户检查发现，拒收他做的非法区块。

一笔交易被包含在一个区块里，接在它后面的区块越多，则被其它有阴谋的分支链替换且交易无效的机会就越小，一般认为经过 6 个区块确认就相当可靠了，简称为 6 个确认。6 个确认的等待时间为一小时左右，也就是比特币汇款到帐的时间。

【6 页确认】：6 个区块确认可以比喻为 6 页帐单确认。

理论有一种方法对比特币系统发起攻击。攻击者需要有很大的计算力，超过系统的 50%。他们先从自己的帐户里转出一笔比特币，转到交易平台或商店，用来兑换成美元或购买商品，这笔交易是公开的。同时他们开始做区块，不包含自己的公开交易，而包含另一笔不公开交易——把自己帐户的币转到自己的另一个地址或再转到其它平台或商店兑换美元或购物。做出的区块也暂不公开，是秘密链。公开交易被别的矿工制造的区块所包含，经过 6 块确认，交易平台或商店认为相当可靠了，就向他支付了美元或发货。这时攻击者公开自己的秘密链，因为它的算力更大，链更长，系统就判他的链有效，别的矿工做的短链被抛弃。他原来不公开的交易有效，而原来公开的交易因为余额不足而失效，交易平台或商店刚收到的币也被撤回了。这被称为 51%攻击，达到双重支付的目的，即攻击者的比特币被花费了两次。

【51%车队作弊】：51%攻击可以比喻为 51%车队作弊。攻击者需要有超级强大的车队，总体实力超过系统的 50%。做秘密链可以比喻为隐身赛车（假设有隐身技术），做秘密帐单，别人看不见。攻击结束时收起隐身术，公开自己的秘密帐单。因为它的车队更强大，帐单页数更多，系统就判他的帐单有效，其它赛车手做的帐单因为页数更少被抛弃。

比特币自诞生以来，尚未有过成功的 51%攻击。大多数矿工是诚实的，而且目前比特币的算力巨大，一般个人没有攻击的能力。或者在经济角度来看攻击也有风险，诚实的挖矿赚

取收益更可靠。但在理论上，某些政府或大财团有发起攻击的能力与动机。

比特币获得了很大的成功，在 2010 年它首次公开交易的市场价为 1 个比特币兑换 0.03 美元，到 2013 年 11 月最高达 1 个比特币兑换 1242 美元，一度超过一盎司黄金的价格。

新技术发展动态：

去中心化货币的发展没有停息。在比特币之后技术创新的典范是未来币，英文名称是“Nxt”，货币代码“NXT”，诞生于 2013 年 11 月。它继承了比特币的区块链等技术，使用创新的纯股权证明（纯 POS）与透明锻造机制，以及许多扩展功能，拥有更优秀的特性，被称为第二代去中心化货币。

未来币的持币用户用自己的私钥对上一个区块签名再做散列计算，取前 8 个字节获得一个随机的“hit”值。

【股东抽签】：持币的用户相当于股东，获得“hit”值可以比喻为抽签，每支签写着各不相同的数字。抽签在会议室进行，每个人的桌上都有一个签筒。

同时系统产生一个“目标值”。每个用户的目标值不同，与各自的帐户余额成正比，而且每过一秒数值翻倍。最先是谁的“hit”值小于他的目标值，他就获得了一个区块的制造权。

【股份、抢答】：每个人的帐户余额即股份，获得区块制造权可以比喻为抢答。会议室有一块大电子屏幕，最初显示每个人的股份数与抽签的数字，股份数每过一秒翻一倍（例如你有 1 万个币，一秒之后数字变为 2 万，2 秒之后变为 4 万。当然你实际的帐户余额不会变，下一轮你还是最初显示 1 万个币）。当某个人抽签的数字小于屏幕上他的股份数字，就按下抢答器，获得了一页帐单的记帐权。因为抽签有运气的因素，股份最多的人不一定每次都能最快抢答，但是长期来讲大家运气均等，股份更多的人能拿到更多次数的记帐权。这被称为纯股权证明。

比特币的工作量证明、算力军备竞赛消耗大量而且节节攀升的矿机与电费成本，而未来币的纯股权证明更加低成本、环保、节能。

【无赞助费】：低成本可以比喻为无赞助费。比特币的职业赛车要花费很高而且不断上涨的车辆与汽油成本，全部由股东提供赞助费，赛车手们要卖出大部份的币用来改车加油。而未来币的股东在会议室抽签、抢答，兼职做会计（记帐），非常省钱。如果用省下来的赞助费买更多的自家股票，股价可能更坚挺。

【先有股后有权、不增发】：股权证明，必需先有股后有权。所以未来币的发行机制与比特币不同，全部 10 亿个货币在最初通过 IPO 一次性发行完毕（区块制造者只获得转帐的手续费，每笔最低手续费是 1 个币），象一支永不增发的股票，后来的人通过购买获得。原始股东是 73 个人，单个股东的股份不超过 5%。IPO 募集资金只有 21 个比特币，不够项目开发费用，由原始股东自掏腰包解决，必需做出业绩从股价上涨之中获利。比特币每过十分钟就有新币产出，象一支缓慢但每天增发的股票。增发是给了赛车手，普通人掏钱向赛车手购买获得股票。（纸币本质上也应当是全国人民的股票）

持币的用户是系统的主人，但比特币在工作量证明机制下，可能没有持币的矿工掌握决策权（即算力投票权）与管理权（即区块记帐权）。而未来币在纯股权证明机制下，用户即矿工，更合理。

【员工】：比特币矿工可能没有持币，他们的利益与公司利益部分一致，可以比喻为员工，由员工行使决策权并管理财务部。而未来币在纯股权证明机制下，股东大会行使决策权，股东轮流兼任财务人员，股东利益与公司利益一致性更高，更合理。

比特币挖矿是随机碰撞的，在碰撞成功之前都不能预知谁将获得当前区块的制造权。未来币的“hit”值与帐户余额是公开透明的，可以预知是谁最先获得当前区块的制造权，这称为“透明锻造”。

【暗签赛车、明签抢答】：比特币的随机碰撞挖矿可以比喻为“暗签赛车”。赛车手抽的签是暗签，签上写的是天书，谁都看不懂。但上帝看得懂，按每个人抽签的里程给他们设置不同的终点标记。赛车过程中，赛车手不知道自己要跑多少里程，终点在哪里，直到看到上帝做的终点标记，才知道自己跑完了，成功了。未来币的“透明锻造”可以比喻为“明签抢答”。股东抽的签上“hit”值是明文，而且被公布在大屏幕上，大家看着屏幕报数，可以预知是谁最先获得当前帐单的记帐权。

【抗 90%股东作弊】：安全第一。比特币部分解决了双重支付问题，但仍然有 51%攻击的可能，某些政府或大财团要发起攻击并不难。未来币的纯股权证明、透明锻造机制可以抵御 90%攻击，即抗 90%股东作弊，可以认为杜绝了双重支付的可能。收购 90%的币在现实中不可行，既使收购之后也会失去攻击的动机，因为那时它就成了超级大股东，变成自己攻击自己了。

去中心化更好：去中心化是灵魂。因为算力军备竞赛，比特币的矿机越来越强大而且昂贵，一般人买不起，这导致了算力一定程度的中心化趋势。矿池又趋向于“越大越好”，许多时候两大矿池的算力超过 51%。虽然算力并不都是矿池主的，矿工可以将算力自由撤出，但市场还是有些担忧。而未来币的币人人可买，目前单一用户的股权最大不超过 5%，在纯股权证明机制下，去中心化水平好于比特币。

因为不能预知谁将获得比特币的当前区块制造权，用户只能把转帐信息广播给任一节点，再通过 P2P 网络转发，使每个节点都收到全部的转帐信息。这加大了各节点的网络流量，系统只有每秒最多处理 7 笔交易的能力。因为可以预知谁将获得未来币的当前区块制造权，用户的转帐信息可以直接发送给该节点，更快捷，减少了网络流量，系统拥有每秒最多处理上千笔交易的能力。

【汇款申请单、转单、汇款单处理能力】：转帐信息可以比喻为汇款申请单，转发转帐信息可以比喻为转单，交易处理能力可以比喻为汇款单处理能力。因为不能预知比特币赛车谁将最先跑到他的终点，用户们只能在跑道旁边把“汇款申请单”交给任一赛车手，然后赛车手再复印转交给附近的其它赛车手（假设每台车都有复印机），直到所有赛车手都收到全部的汇款申请单。这加大了赛车手们的转单工作量，使得系统只能处理每秒最多 7 张汇款单。因为可以预知未来币的股东抢答谁将获得记帐权，其它要帐转的股东可以把自己的“汇款申请单”直接交给该股东，更快捷，减少了转单工作量，系统拥有每秒最多处理上千张汇款单的能力，接近 VISA 的处理能力。这被认为是未来币的核心优势，达到大规模普及应用的条件。

比特币的区块数据库现有 18GB 之大，还在不断增大，这限制了系统的交易处理能力，也使得普通用户不适合做全节点（只能使用轻型客户端）。而未来币的区块尺寸（block size）很小，如包含相同笔数的交易，block size 约只有比特币的四分之一。

【帐本大小】：区块尺寸（block size）可以比喻为帐本的大小。比特币的帐单是用毛笔写的，比较大，复印慢，影响了汇款单处理能力。因为房价高，普通人都住小房子，不适合保存完整的大帐本，只能每次要转帐时去大户家借看完整的帐本。而未来币的帐单是用钢笔写的，如果记录同样笔数的转帐交易，帐单大小约只有比特币的四分之一，复印快，汇款单处理能力更大。普通人也可以在自己的小房子里保存完整的帐本。

【航空母舰+舰载机】：比特币目前只是一个基础的货币系统，可以比喻为航空母舰。未来币则除了基础的货币系统，还有许多扩展功能，可以比喻为航空母舰+各种舰载战机。

已规划的扩展功能如下：

●去中心化资产交易（已完成）——在未来币系统中直接交易各种虚拟货币、股票
●别名系统（已完成）——与 DNS 相似
●任意信息（测试中）——可以发送任何形式的信息，包括加密信息
●去中心化计算
●去中心化储存
●即时交易
●混合服务
●多重签名
●服务供应商
●缩减区块链
●智能合约
●双相支付
●投票系统
●信用评判

注：《百喻经》是佛教典籍之一，用 100 个通俗易懂的比喻传播高深的佛学。本文谬称【比特币百喻经】，切勿深究。

码字辛苦，赞助作者：
比特币：1ML4u4TcVKUVwAwE1U9WT1ciUbuQaLfGuo
未来币：4439781282033581600