# 比特币的产生和交易原理

计 21 2012011401 张梦豪

一．简介

比特币是一种虚拟货币（数字货币），最初起源于中本聪（Satoshi Nakamoto）在 2008 年题为《比特币：一种点对点的电子现金系统》的论文（Nakamoto，2008）。在此文中，作者描述了一种完全基于点对点（Point to Point，P2P）的电子现金系统，该系统使得全部支付都可以由交易双方直接进行，完全摆脱了通过第三方中介（例如商业银行）的传统支付模式，从而创造了一种全新的货币体系。它基于一套密码编码、通过复杂算法产生，这一规则不受任何个人或组织干扰，去中心化；任何人都可以下载并运行比特币客户端而参与制造比特币；比特币利用电子签名的方式来实现流通，通过 P2P 分布式网络来核查重复消费。每一块比特币的产生、消费都会通过 P2P 分布式网络记录并告知全网，不存在伪造的可能。

最初，比特币只是作为密码学的创新尝试在一小群极客之间传播，并没有人愿意用现有货币与其进行兑换。经过几年的发展，比特币逐渐进入大众视野，越来越多的商家开始接受比特币。从 2011 年起，随着一系列交易市场的建立，比特币的价格也开始迅速攀升。截至 2013 年 11 月底，比特币的价格一度达到每单位 1200 美元，而其人民币价格也突破了每单位 7000 元。

二．重要概念

（1）hash 散列（SHA256）

散列函数的功能是将任意长度的不同信息（例如数字、文本或其他信息）转化为长度相等但内容不同的二进制数列（由 0 和 1 组成）。比特币采用的是 SHA256，任意长度的信息输入通过这个函数都可以转换成一组长度为 256 个的二进制数字，以便统一的存储和识别。256 个 0 或 1 最多可以组合成$2^{256}$个不同的数，这个庞大的集合能够满足与比特币相关的任何标记需要。此外，任意两个不同的信息输入，想要通过 SHA256 产生相同数字输出的概率，可以说微乎其微。因为输入信息的微小变动将会导致输出数字的巨大变化。这就保证了输入信息与输出数字的一一对应。最后，散列还有一个重要特征，即想要通过输出数字来反推出输入信息，这是极其困难的。因此，如果想要生成一个特殊的输出数字，就只能通过随机尝试的办法逐个进行正向运算，而不能由输出结果逆向推出输入信息。这个特征是比特币能够顺利运行的重要基石。

（2）工作量证明（Proof of Work）

倾注了更多更复杂劳动的事物具有更高的价值，这是比特币运行的哲学基础。对比特币而言，挖矿（Mining）也是使用随机数进行工作量证明的过程。用前一个 block 的 hash 值，加上当前所有尚未封装的交易记录，再加上一个随机数（使得整块数据的 hash 值具有符合要求的开头），这样的计算需要不断的修改随机数

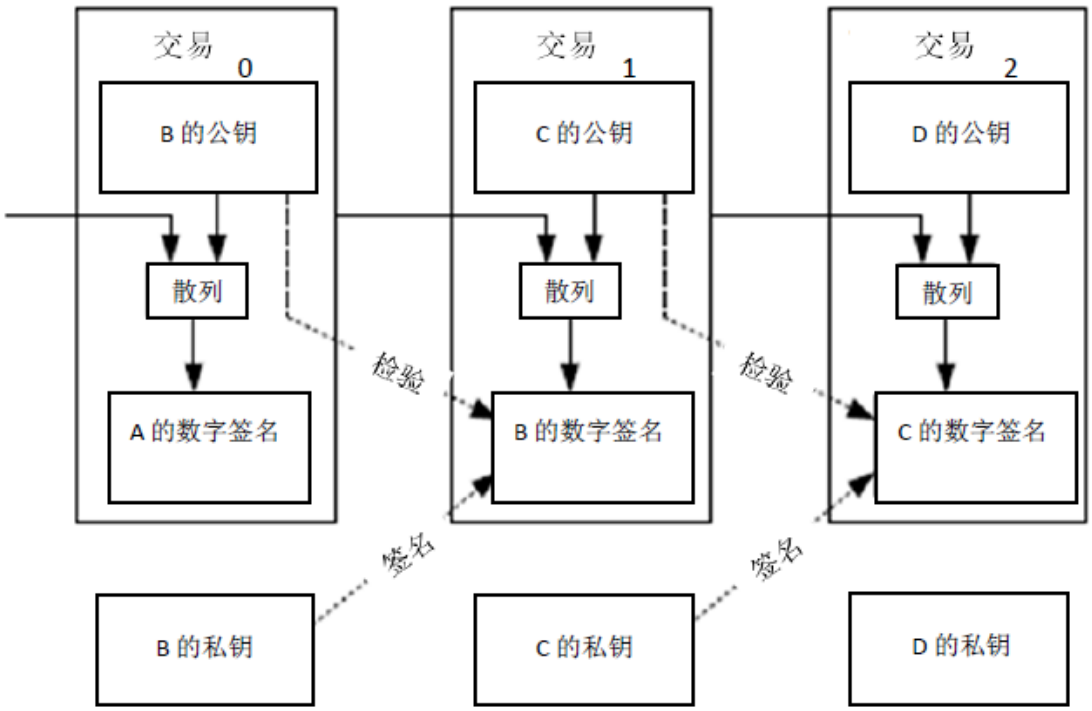
以符合要求，把每个区块完成的时间被控制在 10 分钟左右，随着计算机速度和全网算力提升，寻找特定 hash 头的速度会变快，那么比特币客户端会自动增加特定 hash 值的开头的位数，即提高难度，让每个 block 建造时间始终维持 10 分钟左右不变。这种过程虽然从表面上来看没有产生任何价值，但却是解决互联网中信任问题的有效办法，是在不可靠的网络环境中一种较为可靠的信用证明。

（3））公开密钥密码体系

在信息传递过程中，发送方通过一把密钥将信息加密，接收方在收到信息后，再通过配对的另一把密钥对信息进行解密，这就保证了信息传递过程的私密性与安全性。而密钥无非是一组数字，通过将原始信息与这组数字放在一起进行特定运算，就能够把信息转换为另外一种格式，从而实现加密。解密过程则刚好相反。在大多数情况下，一组密钥由公钥和私钥组成。私钥由自己保存，公钥则需要向其他人公开。在信息传递过程中，公钥和私钥相互配合，既能够对持有私钥的发信人进行身份验证，也能够确保发信人对自己发出的信息不能抵赖，还能够保证收发信息的完整性、防止中间环节被截获篡改。如果公钥丢失，还可以通过私钥进行恢复。但试图通过公钥反推出私钥的努力，从理论上来讲是基本不可行的，这就保证了私钥的私密性。

（4）交易（Transactions）

交易是指一个用户用比特币向另一个用户进行支付的过程。不过，比特币的交易并非简单的支付货币本身。以下图中的交易 1 为例，如果 B 想支付 100 个比特币（100BTC）给 C，那么 B 不仅需要在交易单上注明金额，而且需要注明这 100 个比特币的来源。如图所示，B 的 100BTC 其实来自 A，是 B 通过交易 0 得到的（交易 0 已经通过了全网用户的认证，保存在所有用户的电脑中）。为完成交易 1，B 需要在交易单上填写的信息包括：一是 100BTC 的来源，此处为交易单 0 的 ID；二是 C 的公钥，也即 C 的比特币收款地址；三是将交易单 0 的内容和 C 的公钥输入散列函数，得到一串数字。B 用自己的私钥加密这串数字，作为数字签名放在交易单 1 中。C 在收到交易单 1 之后，可以通过其中存放的 ID 找到交易单 0，并获取 B 的公钥。C 可以使用该公钥对交易单 1 中的数字签名进行解密。与此同时，C 可以把自己的公钥和交易单 0 的内容，按照同样的方式输入散列函数，并将得到的数字与数字签名解密的结果进行比对。如果比对成功，就可以确定如下两个事实：其一，100BTC 的来源属实。因为交易单 0 中包含了 A 的签名，且交易单 0 是经过全网认证过的，即 A 确实将 100BTC 给了 B；其二，交易 1 的确是经由 B 签署的。由于 B 的私钥是唯一的，他无法抵赖这单交易。




上述过程略显复杂。我们可以换一种不太精确但更容易理解的解释。依然以交易 1 为例，交易单 1 中其实包含以下六种信息：一是交易单 1 的 ID；二是资金的来源，即交易单 0 的 ID；三是 A 对资金的签名，以证明是他把 100BTC 给 B 的；四是资金的去向，即 C 的账号（公钥）；五是资金的数额，即 100 BTC；六是 B 的签名（即 B 用自己私钥进行的数字签名），以证明是他自己签发的交易。由于每笔交易单都记录了该笔资金的前一个拥有者、当前拥有者以及后一个拥有者，我们就可以依据交易单实现对资金的全程追溯。这也是比特币的典型特征之一。最后，当每一笔交易完成时，系统都会向全网进行广播，告诉所有用户这笔交易的实施。

（5）区块（Block）

交易和区块的关系，就如同水和瓶子，属于内容和容器的关系。由于每笔交易是相对分散的，为了更好地统计交易，比特币系统创造了区块这一概念。每个区块均包含以下三种要素：一是本区块的 ID（散列）；二是若干交易单；三是前一个区块的 ID（散列）。比特币系统大约每十分钟创建一个区块，其中包含了这段时间里全球范围内发生的所有交易。每个区块中也包含了前一个区块的 ID，这种设计使得每个区块都能找到其前一个节点，如此可一直倒推至起始节点，从而形成了一条完整的交易链条）。因此，从比特币的诞生之日起，全网就形成一条唯一的主区块链（Block Chain），其中记录了从比特币诞生以来的所有交易记录，并以每十分钟新增一个节点的速度无限扩展。这条主区块链在每添加一个节点后，都会向全网广播，从而使得每台参与比特币交易的电脑上都有一份拷贝。在现实世界里，每笔非现金交易都由银行系统进行记录，一旦银行计算机网络崩溃，所

有数据都会遗失。而在互联网世界里，比特币的所有交易记录都保存在全球无数台计算机中，只要全球有一台装有比特币程序的计算机还能工作，这条主区块链就可以被完整地读取。如此高度分散化的交易信息存储，使得比特币主区块链完全遗失的可能性变得微乎其微。

（6）挖矿（Mining）

如前所述，比特币的所有交易记录都保存在主区块链中。每十分钟就会有一个新区块生成并加入进主区块链，这个新区块中记录了十分钟内全网的所有交易。由于比特币使用的是 P2P 模式，这意味着网络上的每个节点都是平等的，没有一个中心节点可以用来承担交易记录工作。因此，如此重要的交易记录任务交给谁来完成，就变成一个现实问题。而比特币创始人中本聪给出的答案居然是任何人来完成都可以。由于每笔交易完成后都会被广播给全网，因此每个人在对交易的有效性进行验证后，都可以根据这些交易数据生成新区块。但这又引发了一个新问题，即如何让所有人都信任由一个陌生人生成的新区块？这个新区块中是否记录了虚假交易或重复交易？要解决这个问题，就要用到前文提到的工作量证明概念。基本思路是，寻找一个随机数，使得将这个数字与新区块的交易信息一起输入 SHA256 后产生的数字，前面 n 位（比如 n=100）都是 0。此项工作的意义在于，由于将会耗费很多时间，如果一个人进行了这项计算且获得成功，那么他提供的区块很可能是真实可信的，因为花费如此大力气作假得到的好处，远远不计花费同样努力从事真实工作得到的好处。此外，其他所有节点在接收到新区块时，也会对其中包含交易的有效性进行校验，这意味着虚假交易或重复交易很难骗过其他所有用户，这就形成了节点之间的信用保障机制。

挖矿（Mining）就是指产生新区块并计算随机数的过程。具体过程可分为以下六步：第一步，由于网络上的每台计算机都保存有之前的主区块链，某台计算机以其中最后一个区块的内容为输入，计算一个散列值；第二步，该计算机在接收广播来的交易单并逐笔校验交易的准确性之后，把没有被列入之前区块的那些交易进行组合，并纳入一个新区块；第三步，该计算机任意猜一个随机数，其大小和长度没有限制；第四步，该计算机将第一步至第三步产生的数据作为输入，一起放到 SHA256 散列函数中，计算得到一个长度为 256 的二进制数；第五步，检查这个二进制数的前 n 位是否符合要求；第六步，如果该二进制数符合要求，则本轮游戏结束，该计算机会把新区块连同这个幸运随机数一起广播给网络上的其他计算机。其他人在收到这个新区块后，会以同样的方式进行校验。如果结果无误，全网就接受这个新区块，将它连同之前的主区块链一起保存。如果产生的随机数不合要求，则第二步至第六步就会重复进行，直到自己成功或者收到别人发来的新区块。

从上述流程中可以看出，挖矿就是指搜集交易数据并建立新区块的过程。这

个过程虽然重要，却耗时费力，为什么所有参与者都趋之若鹜呢？最重要的原因在于，比特币系统规定，每个成功建立新区块的人都将获得 50 个新比特币的奖励，且该奖励将被记录在对应的新区块里。这 50 个新比特币是系统自动产生的，且得到全网的认同。有趣的是，这种奖励的数额每四年减半，即 2009 年至 2012 年年为每区块 50 个比特币、2013 年至 2016 年为每区块 25 比特币、2017 年至 2021 年为每区块 12.5 比特币，如此不一而足。最终，全系统的比特币容量将达到 2100 万个的上限，至此不再增加。从那时起，为保证主区块链能继续不断增长以确保比特币交易能继续正常进行，每个创建新区块的人，都将从新区块包含的交易单中抽取一定的“交易税”作为奖励。这种新的激励机制将保证比特币交易得以延续。

三．交易原理

（1）发行与信用背书

与美元等国别信用货币不同，没有中央银行负责比特币的发行，也没有政府为其提供信用背书。比特币的发行是通过挖矿来完成的。每一次有效挖矿都将产生新的比特币，直至达到数量上限。比特币的信用，则源自所有参与比特币挖矿和交易的用户所付出的大量计算，以及由此消耗的时间和电力等成本。人们为此投入的劳动越多，就意味着对比特币的认可程度越高。比特币系统是一种互联网环境下的新型信用体系，它既不需要任何历史信用记录，也不需要任何机构或个人提供的信用担保。换言之，比特币主要依靠理论和技术的双重保障来保证其信用：一方面，人是理性的，在诚实劳动所能获得的报酬远高于欺骗时，没有人会花费力气进行欺骗；第二，比特币的特征决定了欺骗是极其困难的。要成功进行欺骗，不仅需要经受其他所有用户的检验，也需要具有高于全网总计算能力 51% 的计算设备。以目前比特币全网累积的计算能力来看，即便是全球最先进的大型计算机距离这一要求也相差甚远。随着越来越多的新增计算力加入，在比特币的世界里，欺骗的难度将变得越来越大。

（2）账户管理

账户管理涉及账户的建立、查询和安全保障，比特币也不例外。对比特币而言，建立账户就是生成一个地址。比特币的账户、地址和公钥等概念是基本重合的。账户就是一个地址（一串数字），相当于银行账户的户名，这当然是公开的。地址是由公钥通过一系列数学计算推导出来的，因此地址仅仅是公钥的另一种形式。有了地址，就可以查询比特币账户的余额。

虽然地址类似于银行账户名，但与银行账户不同，该地址的余额并没有特意记录在某个地方。如前所述，每一枚比特币自诞生之日起的所有交易路径都是可追溯的，都被记录在主区块链中。因此，每个账户的余额都可以通过对主区块链进行计算得到，而不需要单独记录。这种设计看似麻烦，但有着明显的优势：首

先，每个使用者可以拥有的账户数量是没有限制的。随着比特币使用者的不断增多，账户数量也与日俱增，为每个账户单独保存余额是对存储空间的极大浪费；其次，对比特币而言，没有中央节点来保存并管理余额信息，想要保存余额信息，就必须将其合并写入到区块中。否则，全网节点在对新生成区块的有效性进行检验时，就不仅需要对新的交易进行检验，还需要对全网所有账户的余额进行追溯检验，这无疑会显著增加工作量。在传统银行里，储户不能仅仅通过户名就对账户余额进行查询。然而，比特币世界允许上述操作，也即任何人都可以通过计算主区块链而查询任何账户的余额。比特币账号是完全匿名的，且每个人可以有多个账号，这就保证了比特币拥有者的个人信息不可能通过分析账号来获得。因此，即使将余额信息完全公开，也可以保证拥有者的个人隐私。

比特币账户的安全管理与传统银行系统完全不同。比特币的所有公开信息（例如交易与公钥）都保存在主区块链中，而主区块链在所有运行比特币软件的计算机上都有完整备份，因此其安全管理的关键在于用户私钥的管理。私钥与公钥一样，都是一长串无规律的数字，很难记忆。而且，私钥是独立存在的，不能被公钥或其他方式反推出来。由于私钥是用户对账户所有权的唯一证明，因此用户每次使用账户时都需要使用私钥。为方便起见，很多用户通常选择将私钥放在文件中或网络钱包中保存，这就使得私钥文件面临着被窃取的风险。而一旦私钥遗失或失窃，就意味着比特币账户的彻底丢失。为防范上述风险，“纸钱包”、“脑钱包”等方法正逐渐被接受。毕竟私钥只是一串数字，完全可以通过写在纸上或打印出来的方式进行保存。这种原始的办法在互联网时代反而是一种非常有效的方式。脑钱包的工作原理与纸钱包完全不同。用脑钱包生成私钥之时，我们可将一句话或一幅图片输入特定函数中，就可得到私钥，且这一过程可以反复进行。因此，脑钱包就把记忆私钥的负担转化为记忆一句话或一幅图片，从而显著降低了记忆的难度。即便这句话或这幅图片不慎被公开，他人也很难猜测其真实用途。

（3）交易确认

传统银行账户间的交易是由银行负责确认的，通常在几秒钟内就可以完成。但对比特币而言，任何交易都需要得到全网的确认，而且必须最终进入主区块链才能生效。在挖矿过程中，每个节点在收到其他节点发过来的交易后都要进行验证，验证失败的交易被直接丢弃，而有效交易则会进入区块。由于全网在挖矿过程中可能在同一时间段生成很多有效区块，且由于网络时延的存在，不同地理位置的节点产生的有效区块可能包含不同的交易集合。因此最终哪个区块能够成为当前时间段的正式区块而进入主区块链，就成为一个问题。

如果一个节点收到了周边节点发来的两个不同的有效区块，它会将它们都挂在主区块链的最后，形成一个 Y 形分叉。后续收到的区块都会基于这两个区块产生，这使得分叉会继续向后延伸。最终，哪个分叉的长度最先达到要求，就会正

式变成主区块链的一部分，而另一条分叉则会被抛弃。由此可见，一个交易从发生到最终确认，需要等待一段时间。通常来讲，在包含这个交易的区块出现之后，还需要等待 5 至 6 个后续区块生成后，才能确认当前区块是否已经正式进入了主区块链。由于每个区块的生成时间大约为十分钟，这意味着一个交易在发生之后，需要等待较长时间才能够得到确认。这既是比特币自身的一大缺陷，也是 P2P 这种全民投票形式难以克服的弊端。

四．展望

首先，作为货币发展史上的重大革新，比特币在设计中使用的一系列创新思想和方式是值得借鉴的。它的出现是解决当前世界各国货币所面临问题的一种积极尝试，因此受到了全世界的广泛关注；其次，由于比特币在寻求以创新途径解决问题的同时，引入了一些难以调和且致命的新问题，导致市场对以目前形式存在的比特币能否取得长远发展报以怀疑态度；再次，比特币的发展前景取决于其能否顺利完成转型。无论是在其上建立其他应用层级，还是将其作为全球货币改革的一个组件，都需要对它进行重新审视和设计。我们认为，如果设计更为合理，且在实施过程中能更好地协调各方利益，比特币的发展前景虽然路途遥远，但值得世人期待。