# 区块链和金融

**刘万燊**

“区块链是真的。”摩根大通首席执行官 Jamie Dimon 在 2018 年 1 月 9 日对福克斯商业（Fox Business）这样说道。他是不是自相矛盾了？过去他曾称比特币是个骗局。

不，比特币不是区块链。比特币是区块链技术的一项非常聪明的应用，使得比特币能够提供法定货币的功能，即，作为交易媒介和价值储藏手段的功能。

尽管政府和一些大型金融机构对比特币仍然保持警惕，但许多人已经接受了区块链技术。他们在探索如何将这项新生技术用于金融服务。新加坡金融管理局局长 Ravi Menon 于 2017 年 11 月 14 日宣布，新加坡和香港将针对贸易金融建立一个基于区块链的平台。IBM、中国银行、汇丰银行、瑞银集团、星展银行、瑞穗和微软等公司也纷纷开始探索使用区块链技术，以转变贸易金融。

据财新网报道，2016 年 12 月，中国人民银行与工商银行、微众银行及中国银行合作，成功完成了基于区块链的法定数字货币的试运行。《金融时报》报道，英国、新加坡、瑞典、澳大利亚和加拿大也在研究基于区块链的法定数字货币的可行性。如果取得成功，可能会产生深远意义。这种货币将减少流通费用、提高透明度、改变货币政策战略的途径，并且对商业银行业务模式带来重大影响。

正在探索中的区块链技术在金融服务的其他应用包括：跨境支付、股票、债券和衍生工具交易、清算与结算、股票发行、筹款、客户尽职调查法规、创造数字资产，以及监管合规等。从 2017 年初开始，几乎每一天都有金融机构、金融科技初创企业或政府机构启动区块链试点项目的新闻。金融行业似乎对区块链技术的潜力持乐观态度。

当然，这些项目中有许多仍然处于概念验证阶段，或者急需寻找用户。总体而言，区块链仍然处于初期阶段，其最终发展还有待进一步观察。

然而，如果你是金融专业人士，你应该了解这项技术。有迹象表明我们正在跨越概念验证阶段，果真如此的话，金融业很可能会发生重大变革。在如此激动人心的技术浪潮中，你应该激流勇进，千万不要落后了。

**为了帮助各位开始学习之旅，下面我将介绍一些关键的非技术性的区块链知识。**

**什么是区块链技术？**区块链技术本质上是提供一种存储和管理数据的新方法。它建立在数十年的密码学研究基础之上。有两个主要的组成部分：

1. 安全的数字签名

数字签名的作用和手写签名一样。它保证了发送电子消息或者发出电子指令的人确实是他/她声称的那个人。

2. 不可篡改的账本

不可篡改的账本意味着一旦数据已经写入账本，没有人可以改变。作为数据的提供者，你可以证明你的数据未被改动，作为数据的接收者，你可以确信数据未被改动。

在我们分别详细讨论这两个组成部分之前，我们需要了解密码散列函数——支持区块链的基础密码术。

**什么是密码散列函数？**它们是接收任何大小的输入或消息，并返回独特的固定大小字母数字字符串的函数。固定大小的字符串被称为“散列值”（hash value），或者简称“散列”（hash）。

密码散列函数的一个主要特性是，几乎不可能从其散列值往回推算初始输入值。因此，这些散列函数被称为“单向散列函数”。例如，比特币区块链使用 SHA-256 密码散列函数。这个 SHA-256 函数可以将整个百科全书转换为独特的 64 个字母数字字符（256 位散列值），但是无法往回解码。

百科全书的任何微小变动，例如增加一个逗号，都会形成完全不同的散列值。这是我们想要从密码散列函数上获得的一个重要特性——即使输入数据有微小变化，散列值也会以无法预知的方式变化。

密码散列函数是区块链的安全性和不可篡改性的基础。SHA-256 由美国国家安全局设计并于 2001 年发布，作为安全性极高的散列函数而获得广泛认可。现在我们准备讨论区块链的两个主要组成部分——数字签名和不可篡改的账本。

**什么是安全的数字签名？**它必须是像手写签名一样。首先，只有你可以签署这个签名；其次，其他人可以验证这是你的签名；第三，签名不可伪造。提供手写签名的数字副本的数字签名方案通常包含三项操作：

1. 你通过良好的随机化算法一起生成一对私钥和公钥。公钥就像你的银行账号，无需保密。私钥是对应于你的公钥的一个字母数字号码，类似于密码，必须保密。

2. 你使用密码散列函数（H）来“签署”数字签名。通过将你想要签署的消息和你的秘密私钥一起散列，创建出数字签名。

   **H（消息，私钥）=数字签名**

   这个签名取决于消息，每次交易都不同，因此无法对不同交易重复使用（即，不可伪造）。这种对消息的依赖性也意味着没有人可以修改消息，因为改动消息就会改变签名。

3. 别人通过采用另一个数学函数（V）来验证你的数字签名，这个函数（V）将你的公钥、消息和数字签名作为输入，如果你是公钥的真正所有者，则返回“真”，否则返回“假”。

**V（公钥，消息，签名）=真（或假）**

这使别人可以验证你拥有私钥，而无需真正看到它。消息（或交易）的确是来自你。

**如何可以使账本不可篡改?** 创造不可篡改的账本的想法，可以追溯到 Harber 和 Stornetta 于 1991 年提出的方案。根据他们的方案，验证交易为有效交易之后，我们使用密码散列函数来散列交易。我们并非仅仅散列当前交易，而是将之前交易的散列值也包含到该散列中，形成一条链。
有了这个系统，对更早交易的任何改变，例如交易 61，都会使交易 62、63 及所有之后的交易的记录变得无效。通过这种方式，我们向账本添加的每项额外交易，都会增强之前的交易。

代替分别连接交易的一个更有效的方法是，收集许多交易到一个区块里，将区块连接在一条链上。账本的完整性和时间顺序使用密码来加强。

区块链可以由可信管理员来管理。这种区块链被称为“私有区块链”。这里存在潜在弱点：让可信第三方负责验证交易和更新账本。如果可信第三方不可信怎么办？他/她可以擅自修改账本，将某些交易从账本中排除，或者为了换取单边支付而厚此薄彼。2008 年，有人提出了建立分布式账本的众包解决方案。

**什么是分布式账本？**2008 年，中本聪（化名）开发了一种针对比特币区块链的很巧妙的奖励性众包解决方案。该方案不让可信第三方管理账本，而是在比特币奖励方案下，通过比赛解决数学题目，让成员网络竞争来形成新的区块。第一个解决数学问题的成员获得奖励。然后他将广播结果，并提议区块链中的下一个区块是什么。网络成员验证数学题目的解答是正确的，而且提议的区块中的所有交易都有效之后，网络成员将通过延伸他们的区块链并结合提议的区块，作为他们接受的信号。由于每个网络成员都保有一套相同的账本或区块链，账本变成了公共账本，通常也称为“分布式账本”。
带有分布式账本的区块链被称为“公共区块链”。比特币是一种成功的公共区块链。

比特币区块链的共识协议可以用以下的简化步骤进行概括：

- 新交易（消息和发送者的数字签名及公钥）向所有网络成员广播
- 每个成员选择一套新交易来形成一个区块，并验证这些交易的有效性
- 他们比赛解决数学题目
- 获胜者向网络广播他/她提议的新区块
- 他开始创建下一个区块，并收到比特币奖励
- 其他成员通过将该提议的区块结合到他们的延伸区块链中，作为他们接受的信号。在技术上，这将会在他们创建的下一个区块中包括提议的新区块的散列值。

我们可以看到，这种分布式账本的优点在于不需要可信第三方。分布式共识协议之后是网络成员证实新交易/区块。比特币的分布式共识协议，又称“工作量证明”（PoW），从一开始就非常有效。但是，尽管获得了成功，这种协议也存在严重的问题。它需要大量的电力来解决数学题目，要花费太长时间来处理交易。

替代 PoW 的另一种分布式共识协议是“权益证明”（PoS）。在 PoS 中，下一个区块的创建者通常通过他们权益的大小组合（例如，他们持有的币数量）及随机化算法来选择。创建者将提议的区块向网络广播。在大多数网络成员验证所提议区块中的交易后，区块将被追加到区块链中。与比特币的 PoW 相比，PoS 更加节能。然而，批评人士认为这种协议更加容易受到攻击。对更快、更便宜、更安全的分布式共识协议的探索仍然在进行中。

**公共、私有和联盟区块链。**公共区块链，例如比特币区块链，在互联网上运行，允许有计算机的任何人提出交易或加入账本的维护。成员无法单独篡改账本。由于没有中央簿记员，所以不存在易受黑客攻击或发生硬件故障的单点故障。不存在垄断交易费用。
分布式共识使公共区块链变得极度安全，但也使得交易处理速度变慢。隐私也是一个令人担忧的问题。相比之下，私有区块链可以大大加快交易处理速度，而且隐私性也高得多，但是私有区块链无法提供像公共区块链一样的分散化安全性。

最近，越来越多机构在合作开发联盟区块链。这种区块链不是允许有互联网连接的任何人参与账本更新，或者允许唯一的可信第三方来完成此项工作，而是向一些选定的当事方赋予这项责任。因此，联盟区块链在一定程度上也是私有的，提供与私有区块链类似的好处，即，效率和隐私，不过又无需将权力由单独一方掌控。 并且不同的用户可以赋予不同类型的许可，例如，允许一些用户查看账本，但是不允许添加数据。这种区块链对金融机构更加具有吸引力，因为允许它们保留控制权和隐私，同时又享受到这种技术的好处。

总之，公共区块链技术（安全的数字签名、不可篡改的账本和分布式共识协议）为我们提供了一种方法：维持可靠的、不可篡改的、不可撤销的、透明的账本。对于许多金融服务和交易而言，这些特质至关重要。如果我们采用的公共区块链是依赖于网络共识和密码术的无需要可信第三方的系统，那么我们在金融交易中可以不需要可信中介者。这种去中介化，如果发生了，将会显著改变金融业格局。能够应对监管挑战的金融科技初创企业，将抢走传统金融机构的很大一部分业务，而且会使不少传统机构被淘汰。现有金融机构会被颠覆，还是会接受新技术并实现自我颠覆，目前尚不清楚。

参考文献:


- Alex Tapscott, and Don Tapscott, “How Blockchain Is Changing Finance,” Harvard Business Review, March 2017.
- Goldman Sachs Equity Research, “Profiles in Innovation: Blockchain,” 2016.
- Haber Stuart, and Stornetta W. Scott, "How to time-stamp a digital document," Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.
- Johnson, Don, Alfred Menezes, and Scott Vanstone, “The elliptic curve digital signature algorithm (ECDSA),” International Journal of Information Security, vol 1.1 pp 36-63, 2001.
- Nakamoto, Satoshi, “Bitcoin: A peer-to-peer electronic cash system,” 2008.