《金融与发展》深受读者喜爱的“返归基础”栏目终于回归了！我们曾在2015年底时终止了该栏目的更新。在这个栏目中，我们向读者解释他们在日常生活中所遇见的经济学术语。此外，您还可以在www.fandd.org上观看“返归基础”的视频版。

什么是加密货币?

新型货币的利益与风险并存

安托万·布弗雷、维克拉姆·哈卡萨

加密货币如同雨后春笋般涌现出来，其名字也是五花八门，比如：质数币（Primecoin）、达世币（DASH）、Verge币。它们吸引了大批技术人才，其价值波动剧烈。有人认为，这些神秘的计算机代码有朝一日将取代我们现在所使用的货币。加密货币到底是什么？是什么让人们认为它具有价值？要回答这些问题，首先让我们来看看货币是如何演变的。

货币的使用

货币是价值的储藏手段、商品和服务的交换媒介、衡量价值的尺度。在货币出现之前，人类社会直接交换商品和服务——比如，用一蒲式耳的谷物换一头猪。这种物物交换的效率低下。随着社会的发展，出现了商品货币——从贝壳到铜、银、金。一些国家推出了法定货币——这类货币本身不具有任何价值，只是付款的承诺——如在8世纪的中国，由唐朝政府发行的纸币。

最早的法定货币的形式既不稳定也不被广泛接受，因为人们不相信发行者会履行承诺，兑现资金。政府为了购买商品或提高工资，加印货币，引发了通货膨胀（想想一战后德国人用手推车运送现金的场景）。现代央行通过代表政府来调节货币供应量，以维持物价稳定。

记账和账本

金融体系的日益发展和复杂化，对可信的中介机构和会计系统提出了要求。意大利文艺复兴时期的复式记账是一项重大创新，强化了大型私有银行的作用。到了现代，各央行的支付系统已处在顶端。随着银行记账的计算机化，央行的协调作用日益增强。

这些记账是如何运作的？金融机构调整其账户持有人在内部账本上的头寸，而央行则在中央账本中确认金融机构之间的交易。例如，小穆用她在甲银行账户里的钱从小马那里购买商品，而小马在乙银行有账户。甲银行从小穆的账户中扣除相应的金额。央行把钱从甲银行转到乙银行，并在其中央账本上记录该笔交易。然后乙银行把钱转到小马的账户上。如你所见，这个系统是建

设计：THE NOUN PROJECT / MASSUPA KAEWGAHYA

立在客户对央行及其维护中央账本的信用的能力之基础上的，并且确保同一笔钱不会被花费两次。

而许多加密货币却不需要有可信的中央机构。相反，它们依赖于分布式账本技术，如区块链，来构建一个通过网络维护的账本（实际上是一个数据库）。为了确保同一个加密货币不会被花费两次，网络中的每个成员都使用计算和密码学的衍生技术来核实和确认每一笔交易。当分散在网络中的成员达成共识之时，就会将该笔交易记入账本中，从而被确认下来。账本能够完整记录特定加密货币的交易史，而且记录是永久性的，不能被单个实体篡改。这种能够就分布式网络中账户之间的交易的确认达成共识的能力是一个基础性的技术转变。

核实和确认交易的网络成员通常会受到奖励，获得新的加密货币。许多加密货币也是匿名的：货币持有者有两个密钥，一个是公开的，如账号；另一个私密的秘钥则用于完成交易。我们继续推演前文所举事例。如果小穆想用加密货币从小马那里购买商品，为此，她用私密的秘钥发起交易。小穆通过她的公开密钥 ABC 在网络中确认她的身份，小马通过她的公开密钥 XYZ 确认自己的身份。网络成员要核实 ABC 有想要转给 XYZ 的钱，那么需要解决一个密码难题。一旦这个难题被解决了，交易就会被确认，一个代表该交易的新区块将被添加到区块链中，于是钱就从 ABC 处转给了 XYZ。

利益和风险

了解了技术之后，让我们再回到加密货币的起源。第一个加密货币比特币是在 2009 年由一名（或一群）化名为中本聪的程序员推出的。根据 coinmarketcap.com 的数据，截至 2018 年 4 月，已有超过 1500 种加密货币。其中，比特币、以太币和瑞波币是使用最多的加密货币。

尽管加密货币被炒得火热，但它仍不能履行货币作为价值储藏手段、交换媒介和价值尺度的基本职能。由于加密货币的价值波动极大，它们基本不能作为衡量价值的尺度或储藏手段。人们接受的支付方式有限，这也限制了其作为交换媒介的职能。与法定货币不同，大批量生产加密货币的成本很高，因为这需要大量能源去驱动解决密码难题的计算机。最后，分散的货币发行模式意味着没有任何实体支持加密数字资产，因此接受与否完全取决于用户的信任。

分布式账本技术可以降低汇款等国际转账的成本，并促进金融包容性。

加密货币及其基础技术有一定的好处，但也存在风险。分布式账本技术可以降低汇款等国际转账的成本，并促进金融包容性。一些支付服务如今可以让海外转账在几个小时内完成，而不再需要花费几天的时间。该技术可以提供超越金融系统的益处。例如，它可以用来安全存储重要的记录，如医疗记录和土地契约。但另一方面，如果没有中介检查交易的合法性或核实个人身份的话，加密货币的匿名性便会使它们沦为洗钱和恐怖主义融资的工具。如果加密货币影响到央行对货币供应的控制，进而影响到货币政策的实施，那么这最终或将给各国的央行带来巨大挑战。FD

安托万·布弗雷（ANTOINE BOUVERET）是IMF战略、政策和检查部的经济学家，**维克拉姆·哈卡萨**（VIKRAM HAKSAR）是该部的副主任。