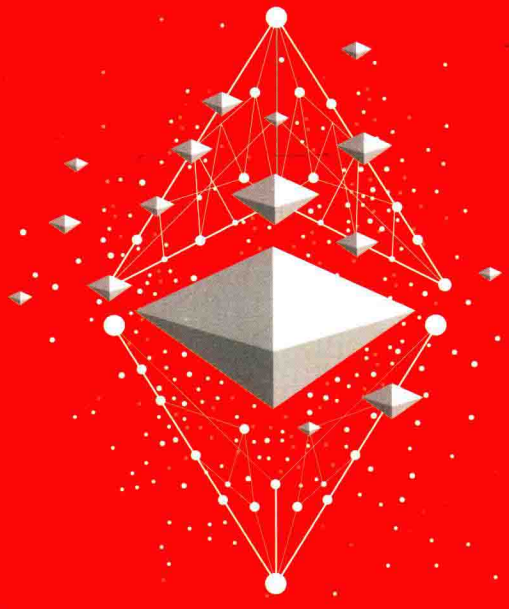
极客起源&51CTO&CSDN&CNBLOG荣誉推荐
100000+读者翘首以盼

本书微视频+价值698元（1800分钟）
JavaScript视频课+本书实验软件+案例
源码+一对一问答+其他不定期惊喜资源

超级学习礼包

李宁◎编著



第一行代码
以太坊

宁哥教你亲手实现你自己的“数字货币”——区块链+以太坊+智能合约+DApp

- **骨灰级大牛：** CSDN超人气博主、51CTO学院金牌讲师、宁哥教育创始人、著名码农李宁亲著
- **全套式服务：** 本书微视频+价值698元的JavaScript视频课、疑难解答、学习资源（开发软件、代码），一扫即得
- **全栈的知识：** 区块链、以太坊、智能合约、DApp，从概念到实战，一站搞定
- **颤抖的成就：** 从入门到实战，带你亲手实现一个属于自己的“数字货币”

中国水利水电出版社
www.waterpub.com.cn

第一行代码——以太坊

李宁　编著

中国水利水电出版社
www.waterpub.com.cn
·北京·

内 容 提 要

本书是一本区块链开发技术图书。本书立足实战，深入浅出地从零开始讲解以太坊及相关技术，包括区块链的基础概念和理论、利用以太坊创建私有区块链、编写智能合约、挖矿、Web3.js API、Solidity 语言、Truffle 框架、Ganache 测试节点等技术。本书力求通俗易懂，实例丰富，步骤详细。为了帮助读者巩固基础知识，本书最后还配有两个综合案例分别实现以太坊在金融领域（发布代币）和非金融领域（DApp）的应用。

本书适合于区块链技术的学习者及从业者使用。

图书在版编目（CIP）数据

第一行代码 : 以太坊 / 李宁编著. -- 北京 : 中国水利水电出版社, 2018.8
ISBN 978-7-5170-6797-9

Ⅰ. ①第… Ⅱ. ①李… Ⅲ. ①电子商务－支付方式－研究 Ⅳ. ①F713.361.3

中国版本图书馆CIP数据核字(2018)第202182号

责任编辑：周春元　　加工编辑：刘玉利　　封面设计：李　佳

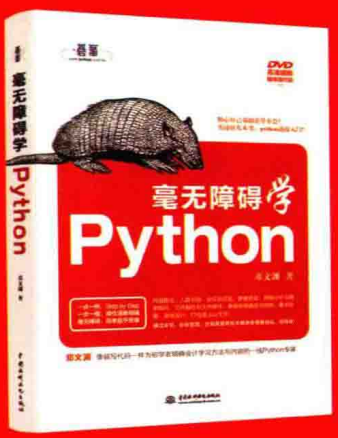
书　名	第一行代码——以太坊 DIYI HANG DAIMA——YITAIFANG
作　者	李宁　编著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市鑫金马印装有限公司
规　格	184mm×240mm　16 开本　20 印张　463 千字
版　次	2018 年 9 月第 1 版　2018 年 9 月第 1 次印刷
印　数	0001—5000 册
定　价	68.00 元

■ 作者简介

李宁

欧瑞科技创始人&CEO，宁哥教育创始人&教学总监，51CTO学院金牌讲师（已录制超过1000小时的视频课程），51CTO、CSDN、CNBLOG博客专家。曾任国内著名软件公司项目经理，企业IT内训讲师，拥有超过15年的企业内训经验和开发实战经验。目前主要从事区块链、比特币、人工智能、大数据、Python、JavaScript、Java、C++、编译器等技术的研究和开发，现在正在带领团队开发支持区块链的跨平台开发系统。曾出版超过30本IT畅销书。

深厚的一线项目开发功力加上多年的培训讲师经历，成就了李宁老师风趣幽默、条理清晰、通俗易懂、深入浅出、实战性强的授课特点。他的课程，经常能够让学生举一反三、发散思维，并指引学生找到适合自己的学习方法。



前言

当今最火的技术是什么？区块链、区块链、区块链，重要的事情说3遍。现在区块链的火爆程度已经全面超过了人工智能。在硅谷，一个区块链工程师有16家公司在盯着。国内某区块链创业公司给出的待遇是“80万年薪+可观原始股（注意不是期权，是原始股）”，就算这样也难以找到合适的区块链工程师。想当年人工智能工程师也没这样吧！由此可见，区块链的技术职位是多么抢手。造成这种情况的主要原因是区块链的理念刚刚诞生没几年，而且涉及到的技术过于庞杂，例如需要熟悉相关的编程语言、底层通信协议、操作系统原理、加密技术等，培训领域很难在短时间内培养出合格的人才，而市场上的人才积累又不多，所以造成了区块链人才过于稀缺。

随着区块链的升温和人才的高度稀缺，不管是想找工作的还是想升职加薪的，都在跃跃欲试，想要分区块链的一杯羹。不过话有说回来，光想是没用的。如果你不会区块链技术，就只能看着别人挣钱了，或者幻想着美好的未来，不过一觉醒来发现只是梦一场。与其光做梦，不如从现在开始学习区块链技术。技术搞定了，钱不是问题，梦想也会变成现实。

作者在博客和公众号（搜索“区块链技术栈”既可关注）上发布了很多与区块链、以太坊相关的文章，经常收到一些读者的E-mail或微信信息，咨询到底如何学习区块链技术，因为区块链技术过于庞杂，里面涉及到的技术非常多，所以让很多想进入区块链领域的程序员感到迷茫。其实区块链技术主要分为应用层（以DApp、智能合约为主）和底层（主要是通信协议、加密算法等）两部分。大多数程序员会从事应用层的开发，少部分程序员会从事区块链的底层开发。这两个层级用到的技术差别很大。例如，应用层会用到JavaScript、Python等编程语言以及Solidity等智能合约语言，而底层会用到C++、Go语言以及通信协议、加密算法等。所以读者在进入区块链领域之前，先要想好要进入哪一个层级。

为了解决程序员对区块链技术感到迷茫这一问题，我决定编写一本探索区块链和以太坊技术、指导开发的书。这本书属于应用级别，如果读者选择了区块链应用开发，那么本书正好可以满足这部分读者的需求。

为什么要选择以太坊作为区块链的学习载体呢？因为以太坊代表了区块链2.0，而比特币代表了区块链1.0。区块链2.0和区块链1.0的主要区别就是扩展性。由于以太坊支持用Solidity语言开发智能合约（一种运行在以太坊网络上的程序），这也让以太坊拥有了无限扩展性，同时也降低了使用以太坊的难度。

本书讲解了区块链和以太坊的核心理论和基本概念，并深入讲解几个与以太坊相关的技术，包

括 geth、Web3.js、Solidity 语言等。同时提供了两个真实的实战案例，以便让读者更好地理解如何编写基于以太坊的应用。相信读者通过本书的学习可以轻松快速地学会以太坊和 DApp 开发。

本书是我将多年软件开发和培训授课经验应用于以太坊技术课程方面的最新实践。本书旨在以通俗易懂、随学随练、分秒有进的方式，使读者真正进入区块链技术的殿堂。

本书的很多知识点及案例都配备了专门录制的微视频，以期能够让读者更方便快捷地理解与掌握相关的知识和开发操作。本书配备了全面的学习及技术支持资源。扫描图书中的相关二维码，可获得相关学习视频资源、习题或练习资源、代码资源、相关实验软件资源、技术支持资源，所有资源均会根据情况及时更新。当然，对于本书读者，等待您的，还有更多惊喜。

超级赠送资源：

本书配备了超级的学习资源。除本书的视频课程外，李宁老师还把与本书紧密相关的价值 698 元的 JavaSctipt 完整视频课程免费开放给本书读者，并且享有与李宁老师一对一交流的机会，还有不定期的免费惊喜。本书资源清单如下：

- 本书的视频课程
- 价值 **698 元**的 JavaScript 视频课程（**绝非让人看半截就要付费的那种**）
- 本书相关实验软件
- 作者一对一问答
- 本书案例代码

扫描下面的二维码，可通过指导获取以上资源。

编 者

2018 年 6 月

目录

1 区块链的基本概念与应用场景

本章将带领大家进入区块链的世界，区块链是现今炙手可热的技术。那么到底什么是区块链呢？区块链有什么用呢？这些问题的答案将在本章揭晓。

通过阅读本章可以：

- 了解 DApp 的基本概念
- 了解什么是比特币
- 掌握什么是工作量证明（PoW）
- 掌握什么是股权证明（PoS）
- 了解什么是 51%攻击
- 了解区块链和以太坊的关系
- 了解超级账本项目
- 了解区块链的主要应用场景

1.1 基本概念

基于区块链的应用与其他类型的应用不同。区块链应用涉及到很多概念，如果不了解这些概念，就根本无法理解相关代码，更别提自己编写程序了。因此，在正式探索区块链之前，先要了解一些必要的概念。

扫描获取学习资源

1.1.1 去中心化应用（DApp）

对于传统的网络应用，都会有一个服务端程序，然后多个客户端连接到这个服务端，这叫作中心化应用。中心化应用必须要保证服务端永远处于可连接的状态，一旦服务端挂掉，就意味着整个网络应用将无法运行（客户端无法连接服务端）。

为了解决网络应用中过分依赖服务端的状况，出现了点对点（Peer to Peer，P2P）应用。在这类应用中并不存在对网络完全控制的中心节点，其中部分节点挂掉，并不影响整个 P2P 网络的运行，

这类应用就称为去中心化应用（Decentralized Application，DApp）。在 DApp 网络中，任何节点都有可能为自己服务，而自己拥有的节点也可以为任何其他节点服务，真正实现了“人人为我，我为人人”的互联网精神。像迅雷下载客户端就属于这类应用。本书主要介绍的区块链就是实现 DApp 的一种重要方法，而比特币是实践了区块链技术的第一个成功案例。关于区块链和比特币的详细描述会在稍后的部分介绍。

理想是丰满的，现实是骨感的。

DApp 的想法非常好，网络中所有的节点互为客户端和服务端。网络中所使用的数据会根据一定的算法将全部或部分数据分布存储在网络中的各个节点上，在必要时会进行数据同步。但是，把数据保存到节点上而非由服务端统一管理，就意味着数据有可能会遭到篡改，某些节点还有可能会发布错误数据。如果是敏感数据，例如比特币交易数据，一旦被篡改，可能会给相关各方造成相当大的损失。因此，发现和防止节点对应用数据进行非法篡改，或者与其他节点分享错误信息是一个重要挑战，这就需要在各个节点对某个节点发布的数据是否正确达成共识。在 DApp 中并没有中心服务器来协调节点，或者决定什么是对、什么是错，因此，这个挑战的难度是非常大的。通常的做法是采用一致性协议（concensus protocol）解决这个问题。不同的 DApp 通常使用不同的数据结构共识协议（一致性协议），例如比特币使用工作量证明协议（PoW）来达成共识。

所有使用 DApp 的用户都需要一个客户端，不过客户端不能直接连接 DApp 网络。在使用 DApp 时，用户首先需要运行 DApp 中自己的节点，然后将客户端连接至节点。DApp 的节点只提供应用程序编程接口，并允许开发者使用 API 开发多种客户端。一些 DApp 开发人员会提供一个官方的客户端。DApp 官方客户端通常是开源的，可以下载使用，否则去中心化的想法就失败了。并且很多官方客户端不仅可以用来操作 DApp，还可以为 web3.js 这样的库连接提供服务，通过这些库可以开发出更强大的 DApp 客户端。

1.1.2 DApp 的内部货币


扫描获取学习资源

对于中心化应用来说，所有者需要盈利才能长期维持应用的运行，因为中心化应用需要支付服务器维护费用、带宽费用、人员费用等。DApp 虽然没有所有者，但与中心化应用一样，维持 DApp 节点的正常运行仍然需要一定的费用，如硬件、网络支持等。因此，DApp 节点需要一些回报来维持运行，于是内部货币登场了。大多数 DApp 都有内置的内部货币，或者说成功的 DApp 都有内部货币，如比特币网络中的比特币就是最著名的内部货币。

那么，每个节点到底应该收多少内部货币呢？这由共识协议决定。根据共识协议，只有为维护 DApp 安全和运行做出贡献的那些节点可以赚取内部货币，只进行数据读取的节点没有回报。例如，在比特币网络中，只有矿工（miner）成功挖矿才能赚取比特币。

1.1.3 比特币


扫描获取学习资源

比特币（bitcoin）是一种去中心化的货币，是最热门的 DApp。它的成功充分展示了 DApp 的强大。比特币的成功大大鼓励了人们创建其他的 DApp。在了解比特币的细节以

及为什么人们认为它是一种货币之前，需要先了解两个概念：账本和区块链。

1. 账本

任何交易都需要记录，而用于记录比特币交易的就是账本（ledger）。那么账本与数据库有什么区别呢？在数据库中，我们可以添加、修改和删除交易。而在账本中，只能添加新的交易，不能修改和删除交易。数据库可以用来实现账本，反过来却不可以。

2. 区块链

区块链（blockchain）是用于创建去中心化账本的数据结构。也就是说，区块链与数据库类似，是用于存储数据的。区块链中的区块按序号排列。每一个区块都包含一个交易集合、前一个块的哈希码、时间戳（指明区块被创建的时间）、块奖励、块序号等信息。由于每一个块都包含了前一个块的哈希码，因此可以创建一个互相连接的块链表，所以称为区块链。网络中的每一个节点都会保存一份区块链的副本。

为了保证区块链的安全，工作量证明（PoW，Proof-of-work）、股权证明（PoS，Proof-of-stake）以及其他一致性协议被应用于区块链。由于有这些协议的存在，在区块链中添加新的区块并不容易。例如在 PoW 中，向区块链中添加区块的过程被称为“挖矿”，挖矿从技术上说就是解决复杂的计算难题，那么为什么要解决复杂的计算难题呢？通过 PoW 及其他一致性协议是如何阻止某些节点对整个区块链进行攻击的呢？请读者继续往下面看。

1.1.4 工作量证明（PoW）

扫描获取学习资源

工作量证明就是在修改区块链之前先证明你没有对 DApp 网络进行攻击，那么怎么证明呢？就是在本地先完成一项艰巨的任务，然后将完成的结果上传到 DApp 网络进行验证。这项艰巨任务不能让人用投机取巧的方式来完成，而必须用最原始、最暴力的方式一点一点完成，完全是拼体力。

那么可能有很多读者会问，完成任务和阻止攻击有什么关系呢？这就涉及到一个经济学的概念——经济惩罚。大概的意思就是既然无法阻止攻击，那么就让攻击付出惨重的代价。

完成 DApp 网络交给你的任务是要付出代价的。通常的任务是解决计算难题，这种解决计算难题的过程被称为“挖矿”。

在 PoW 中要解决的难题通常是计算一个哈希值。例如，给定一个基本字符串“Hello, world!”，我们的任务是在这个字符串后面添加一个名为 nonce 的整数值，对变更后的字符串进行 SHA256 哈希运算。如果得到的哈希结果（以十六进制的形式表示）是以 0000 开头的，则验证通过。为了达到这个工作量证明的目标。我们需要不停地变化 nonce 值，对得到的新字符串进行 SHA256 哈希运算。按照这个规则，我们需要经过 4251 次计算才能找到恰好前 4 位为 0 的哈希散列。我们发现，随着 0 的个数增加，计算难度会以指数级增加。而且没有算法可以立即算出结果，但结果却是非常容易验证的。所以要完成这项任务，就需要非常强的算力，也就是说，要想搞定这个任务，需要自己花钱买一大堆高性能的计算机。而且现在区块链分派的任务越来越艰巨，计算量越来越大。如果是以营利为目的的攻击，为了价值几百万的比特币，你可能要花几千万去购买计算机来完成相关的

计算任务，完全是得不偿失。所以很少有人去做这样的赔本攻击，因为攻击成本远大于收益。


扫描获取学习资源

1.1.5 股权证明（PoS）

PoS，简单来说，就是根据持有货币量和时间来分发利息的一个制度。在股权证明模式下，有一个名词叫币龄，每个币每天产生 1 币龄。例如，你持有 100 个币，总共持有了 30 天，那么，此时你的币龄就为 3000，这个时候，如果你发现了一个 PoS 区块，那么你的币龄就会被减去一定的值，每减少 365 个币龄，将会从区块中获得 0.05 个币的利息（可理解为年利率 5%），那么在这个案例中，利息 = 3000×5% / 365 = 0.41 个币。要注意的是，5%的年利率仅仅是作者举例，并非每个 PoS 模式的币种的年利率都是 5%，比如点点币（PPCoin）就是 1%年利率。


扫描获取学习资源

1.1.6 51%攻击

由于区块链分配的任务难易程度不同，可能有很多人会想对策，我不用那么大的计算量，少买点计算机，是否可以找到一个盈利的平衡点呢？其实一开始我也是这么想的，但根据 PoW 算法机制，如果你的计算量不够大，是无法控制区块链的走向的，也就是说，即使你投入了大量的成本用于完成任务，也不能保证自己成功。这就像花了数百万购买彩票，你只能保证比只花两元钱购买一张彩票的人的中奖几率大，但并不能保证你一定能中奖。花几十万上百万就中袋洗衣粉，花两元中 500 万的也大有人在。彩票奖金的设置永远要远小于购买所有彩票的成本，所以你是无法采用穷举的方式保证 100%中奖率的。区块链也是一样，即使你的算力非常强，也不能保证 100%成功，只是成功的可能性更大而已。

前面说过，谁的算力强，谁最先解决问题的概率就越大。当掌握超过全网一半算力时，从概率上就能控制网络中链的走向，这就是“51% 攻击”。这也是区块链的弱点，谁掌握了超过全网一半的算力，谁就可以主导区块链网络。也就是说，区块链并非 100%安全，但如果要蓄意攻击区块链网络，则需要付出很大的代价。那么区块链受到攻击也只能存在于理论层面。


扫描获取学习资源

1.1.7 以太坊

以太坊是一个去中心的平台，允许在这个平台上运行 DApp。DApp 需要依赖智能合约，而智能合约要使用 Solidity 语言编写。一个或多个智能合约可以一起组成一个 DApp。因此，运行在以太坊上的程序就是智能合约。

我们可以将以太坊比喻成 Android 系统，而智能合约就相当于运行在 Android 系统上的各种底层的库。后面的章节会讲解 web3.js，它是用于调用智能合约的 JavaScript 接口，相当于 Android SDK。也就是说，可以使用 JavaScript 编写客户端来调用智能合约程序，使用 JavaScript 接口编写的区块链客户端就相当于 Android 系统上的 App。

智能合约之所以要运行在以太坊网络上，是因为运行在以太坊网络上的智能合约非常容易彼此交互，有了智能合约，开发人员并不需要为集成各种共识协议和其他东西而操心，这些以太坊都可

以轻松为我们搞定，而开发人员只需要编写应用逻辑代码即可。

以太坊有一个内部货币，叫以太币（ether）。为了发布智能合约或执行智能合约中的方法，需要一定数量的以太币。


扫描获取学习资源

1.1.8 超级账本项目

超级账本是一个项目，是首个面向企业应用场景的开源分布式账本平台。在 Linux 基金会的支持下，超级账本项目吸引了包括 IBM、Intel、Cisco、摩根大通、腾讯等在内的众多科技和金融巨头的参与，以及在银行、供应链等领域的积极应用实践。超级账本社区在成立一年多以来，也得到了广泛的关注和飞速的发展，目前已经拥有超过 140 家企业会员。

加入超级账本的有很多项目，Fabric 项目就是最早加入超级账本项目的顶级项目。它由 IBM、DAH 等企业于 2015 年年底提交到社区。Fabric 项目用 Go 语言实现，在 gitHub 上已经有超过 5000 次提交。该项目的定位是面向企业的分布式账本平台，创新地引入了权限管理支持，设计上支持可插拔、可扩展，是首个面向联盟链场景的开源项目。

联盟区块链是指其共识过程受到预选节点控制的区块链。例如，不妨想象一个由 15 个金融机构组成的共同体，每个机构都运行着一个节点，而且为了使每个区块生效，需要获得其中 10 个机构的确认（2/3 确认）。区块链允许每个人都可以读取、只受限于参与者或走混合型路线，例如区块的根哈希及其 API（应用程序接口）对外公开，API 可允许外界用来作有限次数的查询和获取区块链状态的信息。这些区块链可视为“部分去中心化”。

1.2 区块链的应用场景

区块链技术已经从单纯的技术探讨走向了应用落地的阶段。国内外已经出现大量与之相关的企业和团队。有些企业已经结合自身业务摸索出了颇具特色的应用场景，更多的企业还处于不断探索和验证的阶段。

实际上，要找到合适的应用场景，还是要从区块链技术自身的特性出发进行分析。

区块链的主要特点是在不引入第三方中介机构的前提下，可以提供去中心化、不可篡改且安全可靠的机制。因此，理论上，所有直接或间接依赖于第三方担保机构的活动，均可能从区块链技术中获益。

区块链自身维护着一个按时间顺序持续增长、不可篡改的数据记录。当现实或数字世界中的资产需要生成数字摘要时，区块链便成为确权类应用的完美载体，提供包含所属权和时间戳的数字证据。

可编程的智能合约使得在区块链上登记的资产可以获得在现实世界中难以提供的流动性，并能够保证合约规则的透明和不可篡改。这就为区块链上诞生更多创新的经济活动提供了土壤，为社会资源提供更加高效且安全的流动渠道。

在未来几年内，基于区块链的应用将会在各个领域落地，如金融服务、征信管理、资源共享、物联网等。

有理由相信，区块链技术落地的案例会越来越多。这也会进一步促进新技术在传统行业中的应用，带来更多的创新业务和场景。

扫描获取学习资源

1.2.1 金融领域

自有人类社会以来，金融交易就是必不可少的经济活动，涉及货币、证券、保险、抵押、捐赠等诸多行业。交易角色和交易功能的不同，反映出不同的生产关系。通过金融交易，可以优化社会运转效率，实现资源价值的最大化。可以说，人类社会的文明发展，离不开交易形式的演变。

传统交易本质上交换的是物品价值的所属权。为了完成一些贵重商品的交易（如房屋、车辆的所属权），往往需要十分繁琐的中间环节，同时需要中介和担保机构参与其中。因为交易双方往往存在着不能充分互信的情况。一方面，要证实合法的价值所属权并不简单，往往需要开具各种证明材料，存在造假的可能；另一方面，价值不能直接进行交换，同样需要繁琐的手续，在这个过程中存在较多的篡改风险。

为了确保金融交易的可靠完成，出现了中介、担保机构这样的经济角色。它们通过提供信任保障服务，提高了社会经济活动的效率。但现有的第三方中介机制往往存在成本高、时间周期长、流程复杂、容易出错等缺点。金融领域长期存在提高交易效率的迫切需求。

区块链技术可以为金融服务提供有效、可信的所属权证明，以及相当可靠的合约确保机制。区块链技术的出现，被认为是有可能促使这一行业发生革命性变化的“奇点”。除了众所周知的比特币等数字货币实验之外，还有诸多金融机构进行了有意义的尝试。

例如，来自欧洲中央银行的一份报告显示，区块链作为分布式账本技术，可以很好地节约对账的成本，同时简化交易过程。相对原先的交易过程，可以近乎实时地变更证券的所有权。

中国人民银行也对区块链进行了深入的研究。

2014 年，中国人民银行成立发行数字货币的专门研究小组对基于区块链的数字货币进行研究，次年形成研究报告。

在 2016 年，中国人民银行对外发布消息，称深入研究了数字货币涉及的相关技术，包括区块链技术、移动支付、可信可控云计算、密码算法、安全芯片等，这被认为是官方积极关注区块链技术发展的重要事件。

2016 年 1 月 20 日，中国人民银行专门组织了“数字货币研讨会”，邀请了业内的区块链技术专家就数字货币发行的总体框架、演进以及国家加密货币等话题进行了研讨。会后，发布对我国银行业数字货币的战略性发展思路，提出要早日发行数字货币，并利用数字货币相关技术来打击金融犯罪活动。

2016 年 12 月，中国人民银行成立数字货币研究所。初步公开设计为“由中国人民银行主导，在保持实物现金发行的同时发行以加密算法为基础的数字货币，M0（流通中的现金）的一部分由