中国区块链
应用研究中心
嘉楠耘智
鸣金网 MINGIN
联合出品

区块链
探索重构人类社会运行秩序的力量

# 区块链与新经济

## 数字货币2.0时代

高航 俞学劢 王毛路◎编著

全面阐释区块链技术机理
系统解析以太坊生态系统

王 巍 陈心颖 陈九霖 施水才 白 硕
祝慧烨 安青松 石现升 贺 强 周惠东
Vitalik Buterin 韩 锋 孔华威 张一锋

等数十位大咖集体力荐

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

中国区块链
应用研究中心
Canaan
嘉楠耘智
鸣金网
MINGIN
联合出品

# 区块链与新经济

## 数字货币2.0时代

高航 俞学劢 王毛路◎编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

**图书在版编目（CIP）数据**

区块链与新经济：数字货币 2.0 时代 / 高航，俞学劢，王毛路编著. —北京：电子工业出版社，2016.7
ISBN 978-7-121-28830-2

Ⅰ. ①区… Ⅱ. ①高… ②俞… ③王… Ⅲ. ①电子商务—支付方式—研究
Ⅳ. ①F713.36

中国版本图书馆 CIP 数据核字（2016）第 105608 号

策划编辑：刘声峰（itsbest@phei.com.cn）
责任编辑：刘声峰　　特约编辑：徐学锋　　文字编辑：冯　照
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：720×1 000　1/16　印张：35.5　字数：592 千字
版　　次：2016 年 7 月第 1 版
印　　次：2016 年 7 月第 1 次印刷
定　　价：75.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：39852583（QQ）。

# 目 录

PART 2
区块链

附录

# 区块链创业地图

PART 1

# 比特币

第一章

# 数字货币概况

## 第一节 数字货币起源

### 一、早期尝试

1952 年，美国加利福尼亚州富兰克林国民银行率先发行银行信用卡，标志着一种新型商品交换中介的出现。美洲银行从 1958 年开始发行“美洲银行信用卡”。1974 年，罗兰德·莫诺（Roland Moreno）发明了 IC 卡作为电子货币的存储介质。1982 年，美国组建了电子资金传输系统，随后英国、德国也相继研发了类似的系统。以银行信用卡为代表的电子货币迅速流行，成为当今主流的货币形式。

电子货币实现了货币彻底的去实体化，虽然我们仍然会使用卡片作为电子货币的载体，但是卡片本身并不是货币，真正的货币是卡片中所存储的数字。如同早期纸币对应于金库中相应价值的黄金，早期电子货币也对应于银行中相应数额的纸币。但是随着各国货币的发行转向电子化，电子货币也日益与纸币脱离，成为纯粹数字形态的货币。

电子货币是法定货币（以下简称“法币”）的电子化形式，它的发行机制与传统法币相同，资金的传输由金融机构承担和维护。许多人认为这种电子货币存在一些弊端，如无法匿名使用、无法全球流通、交易成本较高等，于是他们开始尝试设计一些新型的电子货币方案（为了与金融系统发行的电子货币相区分，我

们称之为数字货币），例如 20 世纪 90 年代的 DigiCash、b-money、Beez、Flooz 和稍后的 BitGold、ecash。这些尝试有的只限于纸面设计，并未实际实施，而有些实际实施了的也均以失败告终，要么根本没有流通，要么流通的范围极其有限。

失败的原因大多可归结为中心化的组织结构。这些货币由特定组织发行，他们对货币的安全使用与流通进行仲裁、监督和维护，并采用中央服务器记录货币的流通情况。在缺乏国家信用支撑的情况下，一旦发行和维护组织破产或遭受法律、道德指责，或保管总账的中央服务器被黑客攻破，该货币即面临信用破产与内部崩溃的风险。

## 二、技术挑战

如果不使用中心化的组织结构，那么如何对数字货币的流通进行监管就成为一个棘手的问题。数字货币只是一串字符，复制和篡改几乎不需要成本；电子货币在网络中流通，其交易数据最终必然记录于某个“账本”之中，使用黑客技术篡改这些记录也不是难事。因此，无人维护的电子货币系统，其安全性几乎是不可能保障的，这里主要涉及两个问题：

### 1．货币伪造

在中心化管理的系统中，所有用户的账户余额都会记录在中央服务器中，除非入侵中央服务器，用户是无法修改自己账户余额的。如果没有这一中心化管理系统，用户的电子货币存储在自己的钱包里，那么修改余额将非常容易。

### 2．双重支付

中心化管理系统通过实时修改用户的账户余额，可以有效地防止双重支付（用户利用网络延迟等漏洞，把同一笔钱支付给两个人），然而无人监管的系统很难防止这一情况的发生。

早期的数字货币也曾在这两个问题上进行了尝试。例如，B-money 方案提出了一种协议，使用工作量证明机制进行货币发行。每笔货币的传输会广播给所有用户，每个用户都知道别人的账户，因而可以证明交易的真实性和正确性。在网络出错的情况下，用户可以申请赔偿，由第三方进行仲裁，如果仲裁无法达成一

致，则每个用户自行确定自己的赔偿或惩罚额。

BitGold 方案描述了一个使用去中心化方法创建永久工作量证明链的系统，该链记录使用者的公钥、时间戳和签名。该方案认为工作量证明的价值在于稀缺、难以产生、可安全存储与传输。通过点对点的拜占庭回弹（Byzantine-resilient）方法，BitGold 可在传输时防止双重支付。遗憾的是，拜占庭回弹方法依赖于网络地址投票而不是计算力投票，因而容易遭受女巫攻击（SybilAttack）。

而致力于创造匿名数字货币的 DigiCash 方案则使用了盲签名 Blind Signature 算法来切断货币提现与支付之间的联系，首次在数字货币设计中引入了密码学算法。

## 三、比特币的诞生

2008 年 11 月，一个化名中本聪（Satoshi Nakamoto）的人（或者组织）在某个隐秘密码学讨论小组中发表了一篇研究报告《比特币：一个点对点的电子现金系统》（*Bitcoin:A Peer-to-Peer Electronic Cash System*），提出了比特币的概念。中本聪认为："借助金融机构作为可资信赖的第三方来处理电子支付信息，内生性地受制于'基于信用的模式'（Trustbased Model）的弱点。"因此，他希望能创建一套"基于密码学原理而不是基于信用，使得任何达成一致的双方，能够直接进行支付，从而不需要第三方中介的参与"的电子支付系统。对应于现实生活中的现金交易，这个系统需要起到两个作用：一是杜绝伪造货币，二是杜绝重复支付。

发表研究报告之后，中本聪开始着手开发比特币的发行、交易和账户管理系统。2009 年 1 月 3 日，该系统开始运行，中本聪随之构造出第一个区块链，它被称为"上帝区块"，最初的 50 个比特币宣告问世。比特币创新性的设计赢得了很多电子货币行业资深人士的赞许。B-money 发明人戴伟（Wei Dai）认为比特币的发明"意义重大"；BitGold 发明人尼克·萨博（Nick Szabo）称赞比特币是"对世界的伟大贡献"；著名密码破译专家哈尔·芬尼（Hal Finney）称它"具有改变世界的潜力"；来自创业公司 OnlyOneTV 的布鲁斯·瓦格纳（Bruce Wagner）称其为"自互联网问世以来最令人激动的一项技术"。

比特币的诞生，意味着一种新型的、去中心化的、无固定发行方的数字货币

的诞生。本书所述数字货币，均指类似比特币的新型数字货币，并在第一卷中以比特币为例介绍数字货币的基本原理和技术特点。

## 第二节 数字货币原理

### 一、防止货币伪造

对于杜绝伪造货币，比特币的解决方案是保留所有货币的所有流通信息（全网总账本），从而确保了可对每一个货币的来源进行追溯，一直到创造出该货币的那个时刻；每进行一次交易，全网总账本上就多记录一次流通信息，并在点对点网络上进行广播，使得所有节点（参与流通渠道维护的所有计算机）都保存有全部货币的全部流通信息。这样任意一个节点在交易之前就可以轻松发现凭空出现的伪造货币，从而杜绝伪造货币的流通。

### 二、防止重复支付

为了防止同一个货币被同一个人重复花费，中本聪采用了工作量证明法。如前所述，每个交易都要向网络进行广播，重复花费多次就意味着多次广播关于同一个比特币的交易。其他网络节点将把其接收到的其中某一次交易放到一个区块 A 内（一个区块包含了多个近期的交易单）进行验证，验证方法是进行一次耗时的计算，如果计算成功，则向全网进行广播。如果另一个节点在区块 A 的基础上完成了下一个区块 B 的验证，那么它就会把 B 的区块挂在 A 区块之后，依此类推，形成一个区块链。

对于同一比特币的多次交易会形成多个区块链，最终的结果就是哪个链条最长，哪个交易就被确认为有效，其他交易则被废弃。这样就确保了一个比特币只能被一个人支付一次。

## 三、无须第三方监管

通过工作量证明法，比特币还基本杜绝了非法篡改历史交易记录的可能性，因为历史记录一旦被篡改，就意味着某个比特币的交易记录出现了一个新分支，篡改者需要自行对新分支进行验证；与此同时，其他所有网络节点仍在老分支上进行验证，持续构造验证链，除非篡改者拥有超越其他所有网络节点之和的计算能力，否则它的分支增长速度永远无法追上老分支，结果是他的篡改行为必将被宣告无效。

在所有节点上保存全部交易记录，通过耗时的计算对交易进行验证，二者结合起来，就构成了一个安全、可靠的去中心化的支付系统。其本质是把集中监管的工作量交付给一个人人参与的庞大网络，网络中的所有节点都承担监管职责。如欲伪造货币或欺骗其他用户，就是与整个网络作对，因而无法得逞。

## 四、比特币的发行

比特币的发行源于货币流通渠道自身。由于每个比特币的每笔交易都需要进行验证，为了鼓励节点全身心投入验证以维护系统的正常运作，中本聪提出了相应的激励机制："对每个区块的第一笔交易进行特殊化处理，该交易产生一枚由该区块创造者（也就是第一个对交易进行成功验证的人）拥有的新的电子货币。这样就增加了促使节点支持该网络的激励，并在没有中央集权机构发行货币的情况下，提供了一种将电子货币分配到流通领域的方法。""如果某笔交易的输出值小于输入值，那么差额就是交易费，该交易费将被增加到该区块的激励中。"也就是说，第一批比特币可被视为"创世纪"比特币，在被"创造"出来之后进行流通，后续比特币通过验证"创世纪"比特币参与的交易产生，再加入流通渠道，产生滚雪球效应，从而使得比特币越来越多。

但是比特币无法永远增加，由于算法本身的设计，每 4 年产生的比特币数值会减半，因而最终比特币的数量会趋近于 2100 万个。

因为对比特币系统进行维护的人可以通过复杂的计算获得比特币奖励，过程类似于矿工挖矿，因此维护者被称为"矿工"，其维护行为被称为"挖矿"。值得注意的是，"矿工"自带设备（一般为定制化的计算机，又称矿机）、自发参与维

护，因而人数很多且时刻变化，不会形成固定的“第三方监管者”。而在特定的时间间隔内，只有一个矿工能够得到奖励，挖矿的争夺非常激烈，从而保证了系统的安全性和稳固性。

## 五、挖矿

比特币的本质是一个互相验证的公开记账系统，而挖矿的本质则是在争夺记账权。从工作内容来看，“挖矿”是将过去一段时间内发生的、尚未经过网络公认的交易信息收集、检验、确认，最后打包加密成为一个无法被篡改的交易记录信息块，从而成为这个比特币网络上公认已经完成的交易记录，永久保存。

在比特币的世界里，大约每 10 分钟会向公开账本上记录一个数据块，这个数据块里包含了这 10 分钟内全网已被验证的交易。因为所有的挖矿计算机都在尝试打包这个数据块提交，于是最后以谁提交的为最终结果，是需要争夺的。最终成功生成那个“交易记录块”（区块）的人，可以获得伴随这些交易而生成的交易费用，外加一笔额外的报酬。交易费用一般都是转出资金方自愿提供给挖矿者的，因此不是系统新增的货币；额外的报酬是新生成的比特币——前面所说的“比特币的发行”。

比特币的有限性就由“额外的报酬”数量来控制。依据比特币系统的设计，大约每 10 分钟可以生产一个“交易记录块”，最初每生产一个“交易记录块”可以获得 50 个比特币的额外报酬，这意味着比特币网络每天增加 7200 个比特币，但是该报酬每 4 年就会减半，因此最终整个系统中最多只能有 2100 万个比特币。

## 六、区块链

矿工们为争夺记账权所运行的计算，实际上是根据哈希值反向求解随机数。大家比赛的是在 10 分钟内看谁找到一个随机数，这个随机数与上一个数据块的哈希以及 10 分钟内验证过的新交易记录合起来可以得到满足某个条件的最小哈希值。这个值越小，对应的比特币网络的难度系数越高。由于哈希值的结果相当随机，无法预知结果大小，所以只能采取穷举法比拼算力。如果某个矿工 10 分钟内没抢到记账权，就只能等待下一轮的竞争。

之所以在求解随机数时要加上一个区块的哈希，是因为这样所有的数据块就被组成了一条可以从前到后不断验证的数据链条。修改中间任何一个数据块的任何交易记录，都会导致从此之后的所有数据块的哈希无法验证成功，而如果企图修改记录后重新找一个合理值计算出符合条件的哈希重新打包，那就意味着之后所有的数据块都需要重新计算哈希，即使都找到了还必须比整个比特币网络计算得更快，才能让网络接受你的结果，这意味着攻击者要拥有超过整个比特币网络其他部分的计算力，换句话说，要使用超过整个网络50%以上的计算力才能保证攻击有效。

这个数据链条就是狭义上的区块链，或者叫做比特币区块链，又称全网总账本，它永久保存在每个用户的计算机上。只有拥有50%以上全网算力才可能篡改这个全网总账本，比特币系统就是通过“区块链+”“挖矿”的机制实现了货币无法被伪造、交易无法被篡改和双重支付无法得逞的目标。而广义上的区块链则是融合了支撑数字货币所具有的各项技术特点的集成技术架构，我们也将会在第二卷集中讨论。

## 七、计算难度与确认次数

矿工找到一个有效的哈希值后，就会迅速把生成的数据块转发出去，别的矿工收到并认可这个数据块后，就会以它为基础进行下一轮的计算。如果期间收到具有更小哈希值的块，则首先以数据链长度为优先，其次以哈希值更小为优先，抛弃之前的结果，在新的基础上继续进行下一轮计算。

为了自动协调比特币的发行速度，系统根据之前若干数据块生成的平均速度自动调整挖矿难度。如果之前数据块的生成时间低于10分钟，就把难度提高，如果高于10分钟就自动把难度降低。难度提升很简单，就是降低哈希值的下限，由于哈希算法的特性，这会造成计算量的指数级上升，因而会增加矿工计算的时间。

对于某笔特定的比特币交易（主要指转账，即把比特币由一个地址转到另外一个地址），正常情况下，这笔交易的交易单会被打包到当前的数据块中。当某个矿工计算出了满足当前数据块要求的哈希值并广播出去，这笔交易得到第1次确认。其他矿工过10分钟后把新的数据块挂接在当前数据块之后，区块链延长，

每延长一个块就意味着得到的确认加 1。当一笔交易获得了 6 次确认，就可以认为这笔交易已经得到了全网的认同，合法、有效，而且不可撤销。

## 八、客户端钱包软件

在比特币体系里，用户的账户（地址）由本地客户端自动生成，是类似 1Gz9XmfTK4aH89MVXky1QxtyMcG44NqDRv 的一串字符。用户告诉别人这一地址后，对方就可以向该地址转账了。

比特币地址其实是一套非对称密钥对中的公钥，这对密钥通过椭圆曲线算法生成，其独特之处在于：使用公钥加密一段信息后，使用公钥解不开，必须使用私钥才可以解开；同样，使用私钥加密一段信息后，使用私钥解不开，必须使用公钥才可以解开。更加独特的是，根据私钥可以很容易地算出公钥，但是根据公钥几乎无法算出私钥。

因此，用户可以把自己的地址（公钥）告诉别人，与其进行加密通信。例如，用户 A 把自己的公钥告诉 B，然后以自己的私钥加密信息，用户 B 用 A 的公钥解开这份加密信息，并可确认该信息由 A 发出（因为只有用 A 的公钥才可以解开）；用户 B 用 A 的公钥加密信息，用户 A 用自己的私钥解开这份加密信息，并可确认该信息是发给自己的（因为只有用自己的私钥才能解开）。但是用户绝不能把私钥告诉别人，因为私钥唯一确定了地址（公钥）的所有权，而且无法通过公钥计算出来。一旦告诉了别人自己的私钥，就等于把该地址里所存的比特币拱手让给了对方，对方可根据私钥计算出公钥（地址），然后从区块链（全网总账本）中查找该地址关联的比特币信息，并动用这些比特币。

用户账户的地址和私钥都保存在比特币钱包文件里，一般情况下私钥是看不见的，由比特币客户端软件自动进行加密、解密运算。因此，钱包文件必须妥善保管，一旦丢失，钱包里所有地址保存的所有比特币就不安全了，有可能被别人盗走。由于整套比特币体系的去中心化和匿名性特性，比特币一旦被盗，没有任何人有权力或能力找回。

用户账户的地址及对应的私钥均由客户端软件自动生成。由于可使用的地址数目足够多，理论上超过 $2^{160}$ 个，而全世界的沙粒仅有约 $2^{63}$ 个，每粒沙子都可