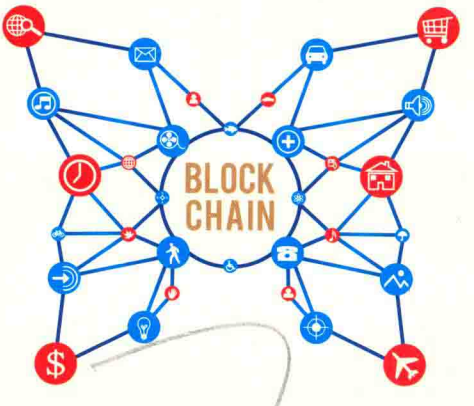
风口区块链

不需要科技知识也能完全读懂的区块链作品



顾炳文◎著

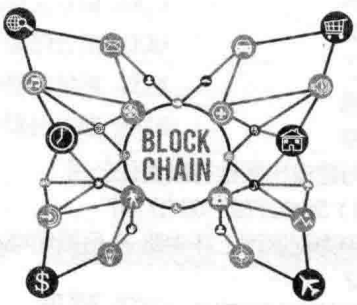
HOW THE BLOCKCHAIN CHANGING YOUR LIFE

民主与建设出版社

风口区块链

HOW THE BLOCKCHAIN CHANGING YOUR LIFE

顾炳文◎著



民主与建设出版社
·北京·

图书在版编目（CIP）数据

风口区块链 / 顾炳文著 . —北京：民主与建设出版社，2018.6
ISBN 978-7-5139-2176-3

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

中国版本图书馆 CIP 数据核字（2018）第 114976 号

风口区块链

FENG KOU QU KUAI LIAN

出 版 人	李声笑
著 者	顾炳文
特约编辑	陈了了
责任编辑	刘 艳
封面设计	刘红刚
出版发行	民主与建设出版社有限责任公司
电 话	（010）59419778 59417747
社 址	北京市海淀区西三环中路 10 号望海楼 E 座 7 层
邮 编	100142
印 刷	北京时捷印刷有限公司
开 本	880mm × 1230mm 1/32
印 张	6
字 数	86 千字
版 次	2018 年 6 月第 1 版 2018 年 6 月第 1 次印刷
标准书号	ISBN 978-7-5139-2176-3
定 价	39.80 元

CHAPTER 1
第一章　在风口上起舞：认识区块链

“站在风口，猪都能飞起来”，小米创始人雷军的这一句话风靡了整个网络。大家心潮澎湃，奋力追逐着新的风口。这个时代什么最火？毫无疑问，是一夜间红遍大江南北的区块链！

“站在风口，猪都能飞起来”，小米创始人雷军的这一句话风靡了整个网络。大家心潮澎湃，奋力追逐着新的风口。这个时代什么最火？毫无疑问，是一夜间红遍大江南北的区块链！

区块链作为一个短时间在网络和现实中迅速蹿红的词汇，对于普通人而言，首先它是陌生的，抽象的，与平日里所熟知的事物存在区别。有的人将其视为一个巨大的商机或机会，也有的人对于区块链存在一定的恐慌，认为区块链可能会对其所从事的行业或工作产生颠覆性的影响。但无论你对于区块链的态度如何，无论它是否会产生这样或那样积极、消极的影响，你都应当对它有全面清晰的认识，来规划指引你未来的生活和工作。

1. 什么是区块链

区块链，作为一项崭新的、跨时代的伟大技术，正不断刷新

着人们的想象，改变着整个世界。历史承载了新技术的故事，无论是蒸汽机、互联网还是区块链，一切技术的演变都充满了机遇与挑战。

区块链（Blockchain），字面意思就是由（交易数据的）区块所组成的链条。区块链，最早且最被人熟知的应用是比特币（Bitcoin）。

比特币，最初由中本聪提出，是一种点对点（P2P）形式的数字货币。点对点的传输，意味着这是一个去中心化的支付系统。比特币不需要特定的货币机构发行，而是根据特定的算法，通过大量的计算产生。比特币在网络交易过程中，可以记录和确认交易行为，且不可随意改变，尤其采用密码学设计，进一步确保交易过程的安全性。由于比特币去中心化的特性，其无法大量制造，也不能人为操控币值。比特币可以用来兑换商品，比如购买虚拟产品，当然只要交易双方认可，比特币也可以购买实体产品。

简单了解了区块链最广泛的应用之后，我们该如何理解区块链本身呢？其实，区块链本质上是一个去中心化和信任化的数据

库，是一连串使用密码学方法产生关联的数据块，其利用数据存储、点对点传输、共识机制、加密算法等，让每个数据块都包含某一段时间内网络上交易的数据信息，以用于验证信息是否有效，并生成下一个区块。可以说，区块链是一个利用去中心化和去信任化的方法，依靠集体来共同维护的可靠的数据库技术方案。

通俗一点说，区块链是一场全民参与的记账，所有的系统背后都有一个数据库，你可以把这个数据库看成一个巨大的账本。当然，这个大账本并非由特定的人来记账，取而代之的是一种软件。我们可以把交易的双方或者多方当作区块链的客户端软件，每个人都在不同的设备上独立记账，而区块链就好似一个巨大的平台，每个客户端所记的账都会在这个平台上展示出来。各方通过这种方式建立联系，加强信任，一旦一方出现问题或者遇到紧急情况，则可以由一个人通知到所有人，避免人与人一对一传话，节省了沟通成本。当然这些人都必须在区块链范围之内。

那么，这样记账能够保证准确无误吗？

首先，我们要明白，区块链属于一种技术方法，可以实现不

同类型的业务，不论大小，不分类别。虽是独立记账，但双方或者多方记账的结果必须保持一致。这就要求记账的双方或者多方必须遵守约定俗成的游戏规则——系统会对客户端软件记账的内容进行统计归纳，以最佳的记账数据为标准，公布给客户端的每个人。每个客户端收到数据后，将自己的记账数据与之进行比对，若匹配，则没有问题；若不匹配，则说明记账有误，需要进行查验纠正，直到符合要求，再记录到自己的账本之中。

可以说，区块链颠覆了传统的网络交易模式。区块链的信息节点在网络上，每个参与的客户端都有机会去竞争记账，参与的人越多，数据越精准。所记账目首先存储在一个数据区块中，记录完毕后对外发布，然后由所有参与人进行核对，确认无误后再记回到自己的账本之中。

对于记账最符合标准的人，因为他们付出了比其他人更多的时间和精力，区块链为其制定了一套奖励机制，同时也鼓励大家在遵守游戏规则的前提下，都争取到这份奖励。

有人提出了新的问题，是否存在冒用他人身份进行恶意破坏

的现象呢？其实这大可不必担心，区块链系统是通过密码算法来实现的，具体来说是通过一种叫公开密钥算法的机制来实现的。密钥分为私钥和公钥。私钥自己操作和保管，而公钥则可以对外公开，交给真正有需求的人。拿到公钥的人并不能直接使用，而是需要通过一系列流程对其进行身份验证，说白了就是需要实名认证才可以使用公钥，否则公钥是发挥不了任何作用的。

公钥的实名认证对那些想投机倒把的人有强大的约束力，那么，私钥是不是没有任何意义呢？其实不然，公钥和私钥必须配合使用才可能发挥其真正的意义。公钥加密的数据要用对应的私钥来解密，同样道理，私钥加密的数据也必须用对应的公钥来解密，若无法对应，即便同时拿到公钥和私钥也是无效的，没有办法使用。这一机制，不仅保证了区块链的规则有序运行，更保障了大家的交易安全。

通过以上介绍，我们大致了解了区块链的概念及应用的基本原理。简单来说，就是大家在一个共同的区域内各自独立记账，然后根据统计分析选出最适合的参照数据，并对每个人的数据进

行验证，保证大家都能够积极、主动、正确地记账。每个客户都有一对密钥，通过系统，在网络中定向发送最有价值的数据，保证双方健康、有序、快速地完成交易。

2. 区块链的分类

区块链的类型主要有公有链、私有链、联盟链、侧链、互联链等，下面将为大家逐一介绍。

公有链

公有链是指全世界任何人在任何时候、任何地方都可以加入，并且可以任意读取数据、发送交易、获得有效确认与认可的区块链，所有人都能参与共识过程。所谓共识过程，就是决定哪个区块可被添加进区块链中并明确当前状态的一个过程。

作为中心化或者准中心化信任的替代物，公有链的安全由共识机制来维护。共识机制遵循每个人获得的经济奖励与对共识过程做出的贡献成正比这一原则，采取工作量证明或权益证明等方式，将经济奖励和加密算法验证相结合。这些区块链通常被认为

是完全去中心化的。

在公有链中，程序开发者无权干涉用户，所以公有链可以保护使用该程序的用户权益。这在传统的经济学角度看来，的确难以理解，程序开发者为何愿意放弃自己的权限？然而，随着互联网崛起，协作共享的经济模式为此提供了两个理由：第一，如果你明确选择做一些很难或者不可能的事情，其他人会容易信任你并与你产生互动，因为他们相信那些事情不大可能发生在自己身上；第二，如果你受他人或者其他外界因素强迫，无法做自己想做的事情，那么，你可以把“即使自己愿意，也没有能力去做”作为谈判的筹码。这就是公有链最大的优势。

私有链

私有链是指其写入权限由某个组织或机构控制的区块链，其读取权限或者对外开放，或者被进行了任意程度的限制。很多人对区块链尚留存私有链有些难以理解，事实上，中心化和去中心化是相对而言的，私有链可以看作是一个小范围系统内部的公有