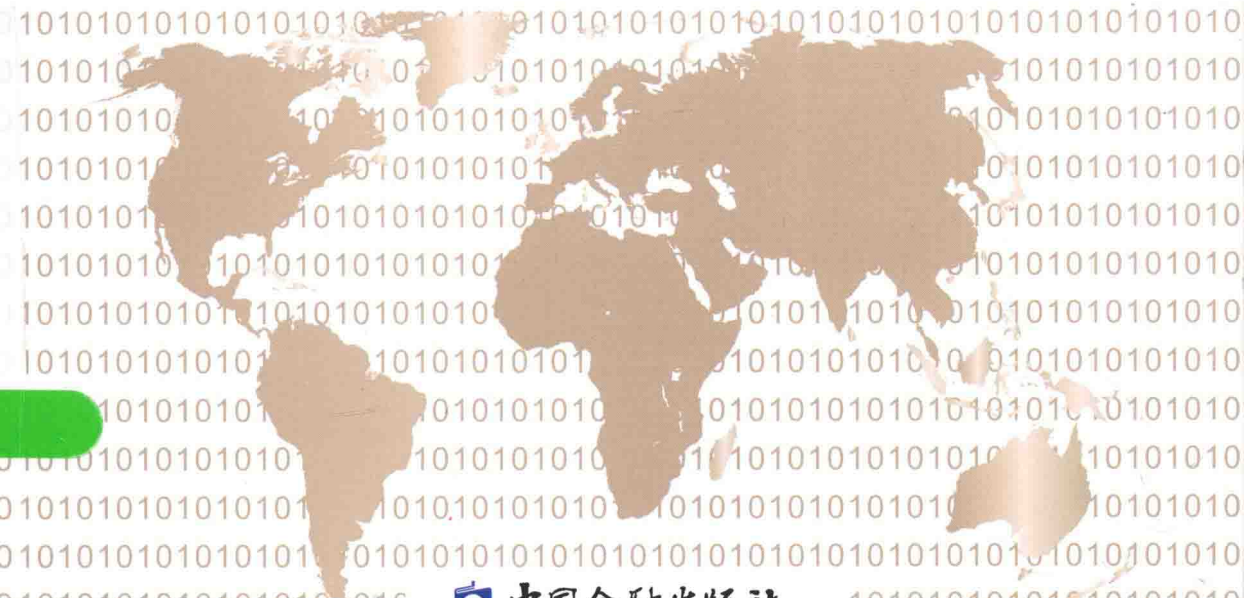
TOMORROW'S TRANSACTIONS

未来交易

戴维·G.W.伯奇（David G.W. Birch）著
柴洪峰　译



中国金融出版社

TOMORROW'S

TRANSACTIONS

未来交易

戴维·G.W.伯奇（David G.W. Birch）著
柴洪峰　译

中国金融出版社

责任编辑：赵天朗
责任校对：孙　蕊
责任印制：丁淮宾

图书在版编目（CIP）数据

未来交易（Weilai Jiaoyi）/戴维·G. W. 伯奇（David G. W. Birch）著，柴洪峰译. —北京：中国金融出版社，2015.6
ISBN 978-7-5049-7317-7

Ⅰ. ①未…　Ⅱ. ①戴…②柴…　Ⅲ. ①电子货币—研究　Ⅳ. ①F830.46

中国版本图书馆 CIP 数据核字（2013）第 319716 号

出版
发行　中国金融出版社
社址　北京市丰台区益泽路 2 号
市场开发部　(010)63266347, 63805472, 63439533（传真）
网上书店　http://www.chinafph.com
　　(010)63286832, 63365686（传真）
读者服务部　(010)66070833, 62568380
邮编　100071
经销　新华书店
印刷　北京松源印刷有限公司
装订　平阳装订厂
尺寸　169 毫米×239 毫米
印张　16.25
字数　225 千
版次　2015 年 6 月第 1 版
印次　2015 年 6 月第 1 次印刷
定价　38.00 元
ISBN 978-7-5049-7317-7/F.6877
如出现印装错误本社负责调换　联系电话（010）63263947

译者序

近年来，互联网金融、移动金融毫无疑问已经成为炙手可热的话题。当传统的金融业与新兴移动互联网产业碰撞在一起，一切将变得皆有可能。

英国 Hyperion 咨询机构专注于电子支付，深入研究智能卡、手机支付、非接触式票据、数字身份等技术领域，曾为肯尼亚 M－PESA 项目提供专业服务。为了借鉴国际同行的丰富经验和发展策略，中国银联把 Hyperion 咨询机构董事戴维·G. W. 伯奇（David G. W. Birch）的博文精选集《未来交易》（*Tomorrow's Transactions*）翻译成中文，介绍给中国金融业和互联网产业的业界同仁以及关注这个行业成长的各界人士。

中国的互联网、移动互联网市场是全球用户最大的市场，发展空间和潜力无限。在线上和线下融合发展的过程中，我们也看到，用户身份信息是其中一个棘手且敏感的问题。正如《未来交易》中反复提到和探讨的，如果能够创造出一种基于特殊算法和加密技术的数字身份，既可以证明用户身份，又不会泄露其隐私信息，相信对互联网金融和支付行业都大有裨益。

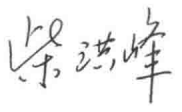
与此同时，货币技术也加快了变革的步伐，这些变化大大改变了传统的交易方式，一系列创新业务遍地开花，甚至超过了创建人的想象。例如肯尼亚建立的庞大的手机支付体系 M－PESA，用户可以通过基于手机短信的应用程序转账，当购物时，用户只需发短信就可以把钱转给卖方。目前，肯尼亚国内生产总值的三分之一流通于 M－PESA 系统，该方案也已被坦桑尼亚、乌干达等其他国家借鉴和使用。

总之，戴维·G. W. 伯奇在《未来交易》一书中描述了数字身份和电子货币未来的发展前景，分析了业务创新与监管力度之间的平衡，阐明了支付和金融业务之间相辅相成，又相对独立的关系。这样一本涵盖了业内多方意见的集成之作，对于正处在高速发展阶段的中国互联网与金融产业，无论从

监管角度还是业务创新角度，都有很高的借鉴价值。

中国银联自成立以来，一直牢记产业使命，履行社会责任，积极响应市场日益多元化的金融服务和支付需求。作为立足中国的国际银行卡组织，中国银联不仅通过与成员机构开展广泛的业务合作，推动建立支付标准，优化改善受理环境，大力推进各类创新支付业务，而且深入开展国内外支付行业研究，了解国内外行业发展的最新动态，总结支付产业特点和发展经验。中国银联将Hyperion咨询机构董事戴维·G. W. 伯奇的博文精选集《未来交易》翻译成中文，推介给国内的金融和互联网行业，希望能给监管机构、从业同仁以及关注这个产业发展的各界人士提供一个有价值的参考。

中国银联董事、执行副总裁



2013年12月

前　言

根据读者对本书2012年版的反馈，我们决定以《未来交易》为题，把关于数字身份、数字货币和数字网络的权威文章集结成册。同样，2013年度论坛的名称也将由“数字货币”更名为“未来交易”。我们还将以“未来交易”为题，重新编辑和发布“数字货币”和“数字身份”博客素材库，为有意了解未来零售交易的人士提供各种形式的宝贵资源。

今年我们对精选的博文稍微做了一些改动，精简并调整了版面布局，但内容仍旧是有关零售电子交易世界的评述和分析。今年的博文集贯穿了几个关键的主题，我想重点提及的是“身份”这一主题，因为它是下一代交易机制的核心。“身份”其实就是“新的货币”。进入2013年，人们在金融、银行、电信、媒体、零售、交通、政府和第三部门构成的超链接世界里到底是什么样的身份，似乎仍无定论。为了明智地选择身份管理基础平台，我们需要对隐私、透明度等关键要点进行深入和广泛的讨论。希望本书有助于这些讨论。

我想再次强调，我撰写这些博文和帖子（由Hyperion咨询机构的其他作者撰写的博文均已注明）的唯一理由，是我的同僚为全球的客户提供了出色的服务，他们有力地支持了交易市场前沿的众多组织机构。本书收集的一些博文汲取了我从全球（包括美国、澳大利亚、法国、意大利、爱尔兰、加拿大以及英国）客户那里获得的灵感。

在此向Hyperion咨询机构的诸位同仁给予的鼓舞谨表感谢。

作者简介

戴维·G. W. 伯奇是Hyperion咨询机构的董事。该公司是一家专注于电子交易领域的信息技术管理咨询公司，主要为世界各地的客户提供专业的咨

询服务。客户包括支付公司、电信运营商、政府机构以及经济合作与发展组织（OECD）等国际组织。1986 年，他协助成立 Hyperion 咨询机构，此前，他曾作为顾问在欧洲、远东和北美工作过几年。他毕业于南安普敦大学物理专业，获得理学学士（荣誉）学位。

在牛津互联网络学会，他被称为“英国互联网和社交网络最敏锐的观察员”，《*Total Payment*》评价他为“欧洲新兴支付体系中的最具影响力者”，《每日电讯报》评价他为“数字货币领域世界领先的专家之一”，《独立报》评价他为“超级怪咖”，金融创新研究中心评价他为“最佳用户友好型英国超级技术专家之一”，《金融世界》称他为“狂人”，他还是“电子金融与支付法规和政策”杂志社的编委会成员之一，*SPEED* 杂志的专栏作家，同时他的创新思维博客和博文在“未来交易”中具有非常大的影响力。

他曾经为 MBA 讲授过新信息和通信技术的影响，多次在《议会 IT 审查》、《瞭望》以及《金融世界》等期刊上发表著作。他是《卫报》的资深专栏作家。他还是一名电子商务问题媒体评论员，曾经接受过“BBC 电视台和电台”、“天空”和其他知名媒体的采访。

英文编辑手记

本书精选来自 www. tomorrowstransactions. com/blog 上发表的博文。对部分原文做了少许删减，印刷版博文集中出现的超链接以参考文献的格式列于文章最后。当然，读者可以在线浏览这些博文，而不必输入尾注中列出的 URL 查阅。本人自行选用收录的博文和评论，并负责撰写各章简介。

简·亚当斯（Jane Adams）

目　录

第一部分　用户

第一章　身份和验证

身份识别问题在电子支付中日益重要。有了功能强大并且能够被广泛接受的身份管理基础平台，就能够较好地解决困扰当前支付市场的一些问题。但要真正建成该平台，还有很长一段路要走。

安全并非数字身份的最佳应用——2012 年 7 月 9 日

谁会傻到公开发送敏感且具有破坏性的电子邮件和即时消息呢？事实上，每个人都会。

在 2012 年 6 月伦敦“互联网身份日”上，人们热烈地讨论电子邮件或文件的安全性对数字身份推广的促进作用有多大，这些内容值得我们深思。几周前我看了 Cory Doctorow 针对 Tom Watson 所著一书[1]中关于 Murdoch“黑客”丑闻的评论，之后我便一直在思考这个问题，人们为什么不对自己的重要通信进行加密呢？

我在报纸上看过一篇类似的评论，它是关于巴克莱银行被曝操纵伦敦银行同业拆借利率（LIBOR）事件的讨论（很抱歉我不记得其出处了）。一位读者提问，为什么银行会雇用这么蠢的交易员，他们明知自己的电子邮件和即时通信日志全都受到监控，还要冒险使用，难道他们真的没有意识到自己的行为是错误的？还是他们不懂得互联网的工作原理？当然，你肯定认为，如果你是想要与同伙合谋的交易员，你肯定会使用隐蔽性高的代码。

那他们为什么不使用安全的方式发送消息呢？至少还能防止其他交易员偷看自己的材料。我知道其中的原因。前一阵子，Hyperion 咨询机构与金融服务类客户合作一个项目，他们希望该项目处于保密状态，要求我们和其他供应商对所有的项目文件都加密并签名，因此大家都重新加载多用途网际邮件扩充协议（S/MIME）。我记得，仅分配证书并将其安装在 Outlook，就用了

好几天。但是运作一天后，客户的IT部门便要求我们关闭加密功能，因为他们的邮件过滤器把所有加密消息都当成病毒过滤掉了。我们只好关闭加密功能，保留签名。可是由于签名与企业的电子邮件网关无法适配，签名功能也只保留了一天。所以到最后，我们又回到最初的状态，仅将文件转换成加密的压缩文件。

我也明白了为什么政府官员会使用明文发送文件。大家都知道这既不符合要求，也让外国机构有机会非法访问我国电子邮件。但问题是，在既没有身份管理基础平台，也没有基于此平台的可行的加密体系的情况下，谁都无能为力。正如“互联网身份日”大会的讨论结果，如果有了身份管理基础平台，问题就变得简单了：你可以通过带备份的密钥给电子邮件加密，法律部门可通过法律程序取得该密钥；然后你再用私人密钥在电子邮件上签名。在这一过程中，私人密钥始终保存在防篡改硬件内，不会泄露。即使黑客、新闻记者或任何其他人登录你的邮箱，他们也无法读取这些加密邮件。这样的话，所有问题就解决了。这也不是什么高深莫测的事，只是缺少身份管理基础平台。当然，这种加密技术并不能完全控制交易员的行为，比如我们还是可能错误地按下“回复给所有人”，导致消息发送给不应该看到这些邮件的人。

那么，大众对电子邮件、即时消息和存储的安全性需求是什么？从互联网早期起，人们就开始关注电子邮件安全问题，但直到现在也没有实现。人们时常提及的“数字邮局”就是建立在安全电子邮件基础上的一个概念。澳大利亚邮政宣布，在2012年4月前，为每个澳大利亚人建立一个“数字信箱”。

或许现在才是适当的时机，但我忍不住想，为什么以前会错过那么多机会呢？毕竟，对身份管理基础平台而言，信息安全并不是什么了不得的“杀手级应用”。许多人嘴上说他们关心安全，却用明文发送电子邮件，在即时通讯工具上讨论犯罪、阴谋这类高度机密的问题，或者把文件放在无密码“保护”的云储存器中。我认为，我们应该关注那些存在身份安全问题的其他领域。关于这一点，Reid Hoffman在《福布斯》上谈到，将来消费者的评

论很可能与他们的购买行为挂钩，通过自动验证评论的真实性，提高评论的价值[2]。

我一直认为，把个人评论和手机钱包连接在一起是个好办法。但为了确保这种联系诚信可靠，需要特殊办法，比如使用假名。当你支付酒店账单时，你的手机钱包会给酒店发送一个电子令牌，酒店签名后返回令牌；手机钱包会给这个令牌解密。在你登录旅行服务公司网站时，你可以把令牌发给他们，从而证明你曾入住酒店。旅行网站、酒店人员及其他看到令牌的人知道你确实在该酒店入住，但你的旅行网站账户仍然可以是匿名的。

这是一种三方共赢的方式，把电子信息放入钱包更加安全。

你无须真正具备“多重身份”，但它的确可以给你带来好处——2012 年 7 月 31 日

谁会对开发匿名身份管理基础平台有兴趣呢？也许是记者。

当我在 TED[3]上看到我曾经撰写的有关数字身份的评论时，我真的很惊讶。我很欣慰当初与同事和客户关于匿名和假名问题展开多次交流，正是这些交流激发了我的灵感。初次讨论这个话题，大家可能会觉得有点深奥，毕竟每个人仅有一个身份的想法已经根深蒂固，没有想过身份是具有范围的。现实不断证明，将基础平台建立在更复杂的身份基础上，可以更好地解决问题，这也说明（至少我这么认为）建立数字身份是大势所趋。

加密技术有什么用处？举一个人物实例，他就是《每日电讯报》雇佣的匿名博主 Inspector Winter，或者更确切地说是幻想家和大骗子 Ellis Ward[4]。报纸需要证明某博主是一名警察，但又不能和第三方合作，证实他的警察身份（如果他的身份暴露了，他就无法再发表博文；但是，他发表博文对社会而言是一件好事）。虚拟身份是如何满足报社的要求呢？它通过一种“盲数法”技术实现。事实上，这个技术既不新鲜，也非创新：自 1992 年 8 月密码学家 David Chaum 在《科学美国人》上发表《实现电子隐私》（第 96 ~ 101 页）的论文以来，迄今已有 20 多年了。在文章中，他写道：

“我开发了数字签名的扩展部分，称之为盲签名，它可以恢复对信息的加密。”

［摘自：“实现电子隐私”[5]］

原理是这样的：Alice 是一名女警察，她利用“盲数”证书证明身份。她首先生成一个随机数，我们称为她的“举报密钥”。她用这个随机数乘以一个只有她自己知道的数，我们暂且称为盲因子，两者乘积形成的数称为盲数。然后，她用警察联合会的密钥签署这个盲数，并发给警察联合会。警察联合会从签名就能判断她是女警察。

随后，警察联合会根据这个盲数制作一个名为“IS_ A_ POLICEOFFICER（是一名警官）”的新证书，用密钥签署后发回给 Alice。约去盲因子后，Alice 便得到一个证书，该证书包含她的举报密钥却又无法追溯到她。

现在，假设 Alice 要向《泰晤士报》证明她是警察。她可在网吧里创建一个 Hotmail 账户，并给《泰晤士报》发送一条用举报密钥和“IS_ A_ POLICEOFFICER（是一名警官）”证书共同签署的消息。《泰晤士报》检查警察联合会的签名的有效性。如果签名有效，他们确认这个密钥的主人是警察。但是，即使《泰晤士报》把这个证书发给警察联合会，他们也无法知晓 Alice 是谁。

当《泰晤士报》想要与 Alice 沟通时，他们可以使用她的举报密钥加密该消息，发到她的 Hotmail 邮箱。由于只有 Alice 拥有这个公共举报密钥的私人密钥，所以她是世界上唯一可以读取该消息的人。不论该消息发布在《泰晤士报》的网站、博客还是其他地方，都没有影响，因为没有人可以解密该消息。

在这种方案下，伪造电子邮件将变得十分困难。因为任何报社可以要求你提供相关的证书来证明身份，比如军警证、护照或者葡萄牙渔业捕捞许可证等。

这看似复杂，其实不然，更重要的是，它很隐蔽。想象一下，你的手机弹出一个菜单，提示你“创建一个新的身份”，然后提供多个身份供你选择，一个人物角色（用于创建假名的身份）或类似上文所述的“举报”身份。

或许这就是一种新型的数字经济，对报纸和其他对真实性要求高的行业而言，它具有重要投资价值。毕竟，这些行业最关心信息的真假，也有保护真实信息的传统。那么为什么不给这些信息来源签发盲证书，使国际开放身份交换组织（OIX）下属的新闻机构互认这些信息呢？

附带数字签名的电子邮件已经存在了很多年，但几乎没人使用。或许，大家认为，与其通过加密来证明你是谁，还不如用它来证明你是做什么的更有意思。

在网络空间里，没人知道你是人还是狗——2012 年 8 月 6 日

现实护照和互联网护照，虽然听着像是一回事，但却截然不同。

在很长一段时间里，我们都在谈论实名、真实面孔等。但有一个更大的问题潜伏在互联网前沿——“蠕虫”，这也是我一直感兴趣的问题。

没人知道你是人是狗，没人知道你是否真的存在，其实这些都不重要，或者进一步说，你是否真的存在这个问题本身也不重要。但实际上，对很多人来说，这确实是个重要问题。

最近，纽约一家专为艺术家和音乐家提供网站解决方案的公司，Limited Run 在其公司主页上发布了一个帖子，声称他们 Facebook 上广告的点击率，有八成来自蠕虫病毒。

［摘自：“广告商控告 Facebook 涉嫌点击率欺诈”，*Business Insider*[6]］

所以说这并不是一个学术问题。知道与你打交道的是不是真实的人是极其重要的。为了做到这点，现在只能在输入框里键入一些连自己都不明白的数字和字母。我们或许应该采取更直接的方法。《新科学家》援引 Chatbots. org 的创始人 Erwin Van Lun 的话，“与其费尽心力检测蠕虫病毒，还不如让人们在网上证明自己的身份”[7]。

在一般情况下，Erwin 的说法是错误的：没有人需要为上网提供证明。但在特定情况下，他又是对的。例如，如果人们不能证明自己的身份，我完全有理由并且能够阻止他们在我的博客上发表评论（但实际上，几乎所有在

我博客上的注册账号看起来都是蠕虫）。正如我上面提到的，证明你是人和证明你是谁是不一样的，这就是为什么在前段时间我自信地预言：

毫无疑问，可公开的 ID 有一个最重要的属性，那就是这个 ID 持有者“是一个真实的人”。

［摘自：“数字身份：供应和需求双方共赢”[8]］

再次强调一下，人们在上网时证明自己的身份，同我们不允许“蠕虫”进入某些领域是两件完全不同的事情。Erwin 甚至建议各国政府为本国公民颁发“互联网护照”。

但我可不希望如此，因为这将是一场灾难。如果你必须有叙利亚政府颁发的互联网护照才能登录网站，难以想象在你访问 www. assadout. com 或其他网站后，这个护照还能有效。两种护照从本质上来看就不同，因为普通护照的价值在于它证明你是谁，而互联网护照的价值恰恰在于它不能证明你是谁。或许我们应该改变关于护照的思维模式以适应网络世界。在古代，你得在目的地申请护照，而非出发地。有了它，旅客就能进城门了。

在中世纪的欧洲，这类文件是由地方政府签发给旅客，文件内一般包括旅客可游玩的城镇和城市的列表。一般来说，到海港的旅行基本上不需要文件，因为海港被视为开放的贸易点，但从港口前往内陆旅行则需要文件。

［摘自：护照 - 维基百科，免费百科全书[9]］

因此，为了进入 Facebook 这个“城市”，我应该申请一个 Facebook 的护照。注意，不是密码，也不是票据，而是护照。密码是一场灾难，今后，我会在博客中详细讨论。我认为，护照的不同之处在于，护照必须根据防篡改硬件制作，并能够验明携带人身份。比如，为了得到 Facebook 的护照，我需要证明自己超过 13 岁，这可以通过学校下发的盲签证书来实现。这种证书可以杜绝 Facebook 串通其他人泄露我不愿透露的资料。也许其他网站认可我的 Facebook 护照，也许他们想让我申请他们的护照。比如，为了进入我的英国银行账户，我必须有一个英国金融服务护照。如果我想玩魔兽世界，那么我就得有魔兽世界的护照。

现在，获得一本护照似乎更加容易了。现实世界中的旅游护照也很容易获得。想象一下，一个人必须有数以百计的护照才能游览世界各国，那将是件多么麻烦的事情。但在虚拟世界中，这些都不是问题。我的手机可以轻松存储数百个护照，而且还可以存储更多。

用“自有设备”完成金融服务——2012 年 8 月 10 日

我不想用他们的设备，我想使用自己的设备。

和其他人一样，我对金融服务的身份识别和验证仍然不抱任何希望。在家里登录网银时，我使用加密锁软件；登录手机网银时，我有客户端密码保护（我已经忘了这个密码），或者用另一个密码拨打电话银行中心（这个密码我也忘记了，所以最近一次打电话过去时，我不得不重新回答一系列安全问题）。如果要登录信用卡副卡账户，我需要使用另一个密码。我在银行 A 下的工作账户和在银行 B 下的家庭账户所使用不同的加密锁。

这太令人抓狂了，纯粹就是浪费大家的时间和金钱。我们已经无法厘清到底是怎样陷入这样一个烂摊子，但是从中走出来应该不难。一个重要的原因是，消费者现在都有自己的设备（比如，智能手机和平板电脑），这些设备足以支持强大的身份识别和认证，也不再需要银行提供智能卡、加密锁等。弗雷斯特公司的 Eve Maler（@ xmlgrrl）注意到了这种转变，他把这种转变称为“带上你自己的口令牌”或 BYOT（Bring your own token）[10]。

我不完全认可 BYOT，相比之下，消费者的自有设备更吸引我。不管怎样，Eve 抓住了重点，而且我们每个人都清楚“设备”指什么。

在不改变基础平台的情况下，消费者的电话号码自然就是他们的密钥，这使消费者只需处理一次令牌及身份验证。也就是说，消费者可以以一种简单的、易于管理的方式来使用身份管理基础平台，比如全国互联网可信身份标识国家战略（NSTIC）等。消费者能够：

被获悉在何地登录，并将密码减少为一个，这些优点较易实现。但核心的问题仍然是身份提供者如何证明身份。文件的内容是对的，但问题是如何