第一章
货币革命开始了

一、突然降临的新货币

比特币是货币史上的革命

比特币作为一种新兴的虚拟货币，从一诞生便引起了各界的关注。一时间，各大新闻媒体争相报道。

这是一种基于网络算法的虚拟货币（Virtual Currency）。（叫作“货币”是否合适，关于这个问题，参考第四章第一节。不过，在美国多叫作“暗码货币”Crypto currency，也有人称之为“数字货币”Digital currency。）

谁都可以轻松使用到比特币。首先，在PC端或者智能手机上下载一个叫作Wallet的应用。在网络上的某个银行兑换点支付日元或者美元，就可以得到比特币了。在接受比特币的店铺（大部分是在线商户）进行购物，然后支付相对应的比特币。2014年5月初的时候交易总额达到54.7亿美元（约合5500亿日元）。从使用人数和接受的店铺来看，美国是最多的。

在日本关于比特币的新闻报道，多是与违法网站的交易等负面的东西在一起。而且，在第二节中讲到的MTGOX的破产，加深了人们对它的消极印象。一见到这样的新闻，多数人都会

想到的是“稀奇古怪的、像假币一样的货币到处散播，谁会是背后的利益获得者呢？”而且不得不注意的一个大问题是价格变动非常剧烈。所以很多人的看法是——“这不过是一种金融上的典型泡沫罢了”。

日本的主流媒体似乎也很难把握到底该如何报道比特币。常见的有“完全是全新的事物，对于今后的走向也会继续关注”“有必要对其进行管制、监管”等诸如此类不涉及实质的言论。

这样的评论归根结底，是因为考虑到比特币“没有发行的责任主体，缺失管理的货币是难以广泛使用的”“肯定在技术或者经济层面还存在某种缺陷，如果持有比特币、使用比特币的话，肯定会在某个时刻蒙受损失”。

但是，比特币的出现，是非常重要的发明。因为它的转账成本极低，所以至今为止，很多本来不可能的经济活动已变为可能了。另一方面，它的存在，会对结算制度、通货制度乃至整个国家的存立根基产生深远的影响。

价格变动激烈，这是不容置疑的事实；包含着像经济泡沫一样的要素，这个也没错。但是，如果被这些表面上的问题迷惑了，就会失去追究事物本质的机会。（在比特币出现之后，外界对此没有一个定论，而且流通量很小，所以造成其价格变动激烈。再者，也可以通过多种方式对价格变动进行合理的引导。）

实际上，会受到猛烈攻击的是既存产业和社会制度。不仅如此，从此种意义上来审视比特币意义的研究，据我所知，在

日本国内还没有出现过。而且，关注比特币存在的潜在可能性，这种可能性会给社会带来何种变革等问题，也还没有与之相关的研究问世。

“无论比特币会带来什么，它的出现都是货币史上的伟大革命，显示建立新的社会形式的可能性。”本书正是站在这样的立场上，解释比特币的结构，以及它的出现会给这个社会带来哪些变化。

比特币的中心：“正确”的交易记录

至今为止的货币一直是由国家、中央银行发行管理的，电子货币是在特定的企业中发行并管理。所以，比特币是一种没有发行者和管理者的货币。

那么，它是怎样得以维持的呢？它的核心是叫作 Block chain 的交易记录。数据并不是由一个空间进行一元化管理的，而是公开的，在多个电脑形成的网络中，作为一个整体来维持的。也就是说支持比特币正常运行的是“人”，又叫作对等网络 P2P 系统。

在 Block chain 中，比特币所有的交易都被记载下来，而且这种记录是不存在伪造货币和反复交易的“正确”记录，事实上也是难以篡改的。这是如何实现的呢？其实它是和比特币的核心思想联系在一起的。

总之，比特币是在当下互联网技术进步的背景下与密码学

融合的产物，它是在加密基础上设计的点对点数字货币，采用了非常巧妙的算法。人类使用货币的历史很长，但是这么长的历史却刚刚开始它具有革命性的思想。（这些在第二章中还会详细论述。）

因为 Block chain 具有开源性的特点，所以接收货币的人，可以根据 Block chain 的记载来查询核对交易记录。只要有记载，自己就是比特币的正当持有者，而且，也可以将自己的比特币转赠给他人。

维持 Block chain 运转的行为，并不是志愿者的活动。而是像挖掘一座金矿一样，矿工会以比特币的形式获取一定数额的酬劳，这样就决定了比特币的总量是恒定的。少量比特币交易中会产生一定的手续费，这个也分配给了采矿的矿工。所以，在比特币的总量达到一定限度时，Block chain 的记录就会更新。

比特币是否值得信任，与它的运作结构是否令人信服有关。因为完全是新事物，所以很多人还是会采取观望的态度吧。

微支付引起的社会革命

作为 Mosaic 浏览器的发明者，马克·安德森（Marc Andreessen）今年 1 月在《纽约时报》（*Why Bitcoin Matters* 2014 年 1 月 21 日）写道："比特币使我们第一次有办法让一个互联网用户将一件独一无二的数字财产交易给另外一个互联网用户，且这种交易是绝对安全的，所有人都知道交易发生，

没有人能够质疑交易的合法性。”比特币交易的安全性和低廉的转账、汇款成本，使得许多原本不可能的事情变为可能。各种各样的企业活动和服务都可以在这个平台上得到构建。

现在的转账汇款成本，即使是在发达国家，也达到了汇款额度的 2% - 3%，而如果这项成本变为零的话，带来的影响将会是巨大的。利益率低于这 2% - 3% 的交易（因现有的转账系统而没有成立的交易），从经济效益角度考虑也是能够成立的了。

其中之一，便是微支付（指在互联网上，进行的一些小额的资金支付）。如果这样的平台实现了的话，原本很多不能做到事情都会成为可能。

最鲜明的例子，就是“内容”的收费化。如果收费在一百日元以下，那么内容就会被尽可能地分开出售，这样就会获得广告以外的收入，没有标题广告，内容的质量也会因此得到提高（参照本章第四节）。

互联网普及以来，“内容销售”产业（报纸、杂志、书籍、CD、DVD、电影等）就产生了严重的版权问题。人们认为“内容”是不可能被免费提供的。但是，在微支付成为可能之后，事态就发生了很大的转变。

另外，发展中国家的汇款成本比发达国家还要高。而且，有时因为部分地区没有银行系统，所以无法汇款的情况也很多。而如果能用比特币汇款的话，发展中国家的经济也会有很大的变化（参照第三章的第三节，第四章的第三节）。

汇款成本的降低和电子商务的改变

互联网的普及使网上购物成为可能。但是在日本，面向个人的电子商务市场规模，在2012年约为9.5兆日元（经济产业省，“平成24年年度日本情报经济社会的基盘整备”，2013年9月），这只占个人家庭消费额300兆日元的3%。美国的情况也是如此。

我认为最大的原因就在于汇款成本过高。因为在实体店铺用现金支付的话，就不会产生这个成本（如果用信用卡支付的话，虽然顾客的成本为零，但是加大了店铺的负担）。所以，购买数万日元的日用品，在实体店铺是最便宜的。

反过来说，如果数万日元的汇款成本降低到接近零的话，那么一定会发生很大的变化。引入比特币不需要费用，小规模的店铺也能负担得起，而且可以增加商品的种类。像家电产品和建材等商品在实体店铺中无法大量摆放，而且从店里运送到家中也比较困难。所以，从制造商那里直接运到客户家中是最简单的方法，这些电子商务都可以做到。

但不是所有的支付都可以使用比特币的，对于那些需要看到实物才能决定是否购买的商品来说，去街边的小店用现金购买更便利。

另外，比特币的支付确认要等待大约十分钟，所以即时支付就无法利用比特币，这类交易就需要电子货币和现金来

支付了。

国际汇款用比特币来代替

如果使用比特币，向地球上任何地方汇款几乎都不需要成本，这是件极具意义的事情，但这会带来什么样的改变呢？

我们可以想到它作为贸易结算货币使用的情况。在现在的贸易结算中，信用证结算的手续费要按照银行汇款的手续费（有关如今国际汇款的结构参照第四章的第三节）来收取。如果使用比特币，就没有这方面的成本了。现实中，还有因汇率问题（买入和卖出的差）增加的成本，使用比特币就不需要与外币进行兑换，所以就省去了这一部分的成本。

然而，现状是比特币与现实货币（美元和日元等）之间的交换比率变动较大，而且还存在受到黑客攻击等危险。因此，比特币的持有时间越短越好。这样，它就需要与现实货币进行兑换，要花费一些成本。总成本无法一言概之，但是可以肯定的是比特币所花费的成本比较低廉。现在的国际汇款基本都被银行独占，所以手续费上涨的可能性很大。如果多设立一些兑换所，使他们的竞争变得激烈，那么手续费应该会有所降低。

这样，使用比特币结算的贸易公司就会在竞争中占到优势，因此其他企业也会引入比特币，如果不引入的话，就会在竞争中处于劣势，从而被迫退出竞争。而且对于贸易出口的一方来

说有一个非常大的好处，那就是可以即时收回货款。

随着使用者的增加，会诞生许多相关的服务。因为对方不是个人而是拥有大笔资金的企业，所以这些服务就会以商业的形式出现。例如面向贸易的特殊兑换服务，或者是为防止在与现实货币的交换比率变动中出现损失，进行的期货交易等形式。

关于比特币，个人利用方面比较受关注。但是个人相对于企业对成本并不那么敏感。许多人虽然知道使用比特币更便宜，但却因为惰性而不愿意改变传统的方法。而企业对于成本却非常敏感，如果他们看到了明显的利润，竞争压力又相当大时，他们就一定会采用比特币。

当然，这对于银行来说是一个严峻的事态，因为外汇业务被侵蚀了。2012 年全世界的贸易额约为 1500 兆日元。假设包括汇率在内的银行手续费占其中的 4%，那么就是 60 兆日元。如果这其中的 1/10 被比特币占领，那么银行的收入就会损失 6 兆日元。这也许会动摇银行的经营基础。

二十世纪九十年代以后，互联网降低了全球的通信成本，这是一个极具影响的改变。呼叫中心和后勤部的业务开始向印度转移。而日本由于语言障碍，被新一轮的全球化所甩下。但是，汇款是不会有语言屏障的，因此日本在这方面也有巨大的可能性。

社会运动的新形态

安德森在上述的报道中讲述了这样一个事迹：

“大学比赛日”这是一个人气活动，就是在美国的大学足球大赛时，学生们会纷纷设计有特点的标语牌来吸引人们的目光。2013年12月，一名学生的标语牌上写着：HI MOM SEND（妈妈，给我汇款）。文字下面配上了比特币的标志和二维码（二维码中介绍了有关汇款的事项），这个画面还出现在了电视屏幕中。

这名学生本人只是将此当作一个噱头，并没有真的想让谁给他汇比特币。但是，在打出标语的24小时内，他便收到了相当于20600美元（约226万日元）的比特币。看现场直播的人们用手机扫描二维码为他汇了款。这些钱最终都捐给了慈善组织。

安德森说：“这以后，人们都可以拿着二维码通过电视来募集捐款了。”

确实如此。这对于那些对现今选举制度不满的人们来说是梦一般的福音。如果该现象得到扩展，那么政治体系也许就会发生巨大的变革。

在前言中我们介绍过，我们在网上会看见这样的照片，在与俄罗斯常年发生纷争的乌克兰街头，路障旁边的市民们都会立起“我们需要援助”的标语（上面印着比特币的二维码）。在安德森做出“比特币会对政治运动发生影响”这个预言的三

个月后，它就变成了现实。

理解结构的必要性

无论是要否定比特币还是要肯定比特币，首先我们都要正确地了解它的结构，而这并非是件容易的事情。

因为比特币是一种崭新的事物，所以人们会在入口处犹豫不决。许多人认为“如果像宣传语一样的话确实不错，但不可能会有那么好的东西”。

实际上，在互联网刚刚出现的时候，大家也是这样的反应。当人们听到“向世界任何地方传送文章或照片，对方都会立即收到，并且不必花钱”这样的话时，谁都不相信，大家心里想的是“那样虽然很好，但是它不可能成为现实”。甚至有人还曾下结论说：“如果那样，世界就会不得了了。”

但是，事实是互联网成为现实、得到了普及，并且改变了世界。现在同样的事情也在货币世界里发生了。

但用互联网与比特币作对比，也许比较难以理解，因为互联网中有很多专业术语，而且这些专业术语都是最近才出现的，关于这方面的教科书非常少，这会造成大家对比特币更大的混乱和误解。

当然，就算不了解比特币的结构，也可以使用它，但是越了解它的结构就会对它的未来看得越透彻。关于比特币的基本结构我们会在第二章进行详细说明。

二、MTGOX 破产的教训

严重的误报和误解："死了"的是货币兑换处，而不是比特币

"关于我死亡的消息，实在太夸张了。"这是马克·吐温说过的一句名言，实际上逝世的不是他，而是他的表弟。

2014 年 2 月末，比特币的私人兑换处 MTGOX 停止了交易。许多媒体针对此事报道为"比特币停止了交易"。很快，"停止交易""比特币脆弱性的显露"等词语大面积地出现在各大报纸的版面。

许多"有识之士"也做出评论说："不通过中央银行的货币制度是无法维持下去的。"还有些人误认为比特币是一种冒牌的电子货币。据报道，财务大臣麻生太郎说："我早就认为它总有一天会崩溃的，那样的东西是无法长久持续的。"

然而，崩溃的只是一个比特币兑换所而已，并不是比特币本身，这要比马克·吐温的误解情况还要严重。麻生太郎所说的"那样的东西"，是指比特币还是指 MTGOX？我们无从考证。但是联系前后文考虑，应该是指前者。总而言之，这是非常严重的"误解"。日本的媒体混淆了比特币本身和兑换所两者的

关系，并将误解扩大。

这就像是以下这个例子一样：从美国旅行回日本的人，要将所剩的美元在成田机场兑换成日元，而恰巧兑换所因故关闭了，我们能因此就说“美元崩溃”了吗？

重要的是，“兑换所是维持比特币系统（区块链的层叠结构 Block Chain 系统）之外的事物”，兑换所是比特币系统的使用方，并不是比特币的运营方。所以 MTGOX 的破产对比特币的运营并没有影响。

关于这点，我们可以以日元为例进行理解。假如现在有劫匪盗走了银行里的日元。这种情况下，我们能说“因为银行在广义上来说是货币制度的一部分，所以日元显现出了它的脆弱性”吗？

一般情况下，是不会出现这种说法的。只能说受害的那家银行防范意识太差，而日元本身并没有任何责任。不能因为维持日元系统之外的问题而失去对日元本身的信任。

MTGOX 事件也是同样的道理。不能说“因为该公司在广义上是比特币的一部分，所以它的破产就显露出了比特币的脆弱性”。

所谓“系统之外”的问题，就像一个人的钱包被小偷偷了，这是防范意识太弱的个人责任，而并非日元体系的问题。

所谓“系统中心”的问题，就像当大量的日元假币流通到市场的时候，会降低日元的信用一样。

以比特币来说，如果它的中心部分 Block Chain 被攻击，

那么就会产生问题，从而影响比特币的信用。但是现在出现问题的并不是它的中心部分。

MTGOX 破产时，根据 P2P 运行的 Block Chain 没有出现任何故障，比特币的交易当然也在正常进行着。到 Block Chain 的网站可以实时地看到全世界的比特币交易都在顺利地继续着，因此，MTGOX 的破产对比特币几乎没有任何影响。

由此我们可以明确两件事情。一个是 MTGOX 的网站没有很好地防御黑客攻击。《华尔街日报》对此做出了最恰当的评论："MTGOX 还没有成熟，或者说它还没有跟上数字货币的成长步伐。"

另一个是黑客了解了比特币的价值，就不会去偷它们，因为知道即使破坏一个兑换所，也不会损失比特币的价值，所以才不会去攻击它。

如果破坏了 Block Chain，比特币就会变得一文不值，因此黑客也就得不到任何经济利益。"因为有价值所以被偷"这是分析犯罪行为时的一个基本命题。

我的意见是"借口"？

2014 年 3 月 13 日出版的一期《周刊文春》，抓住了我在 MTGOX 破产后发表的关于肯定比特币的言论，对此进行了报道，认为我说的都是"借口"。

一般来说，所谓"借口"是指当事人在做了什么错事或发

表了什么错误言论之后，为了辩白说出的缺乏根据的话语。而我并没有做什么错事，也没有说出任何需要用“借口”解释的错误言论。

只能说该杂志的报道是基于“MTGOX 的破产就是比特币的破产”这种错误思想所产生的。

比特币的确不易被理解。特别是这种没有特定管理主体的系统却能够如此顺畅地运营，对于很多人来说都难以理解。我应杂志的邀请，接受了访问，对此进行了详细的说明。即使这样，他们好像还是没有理解。

但是，他们不理解就会一直问下去，而我也并没有辜负如此认真的采访，努力地解释着。然而，他们却将我的说明认为是“借口”，对此我只能说他们这是一种有悖记者道德的行为。

在此，我对《周刊文春》中后半部分的内容进行一下纠正。第一，报道中说交易所是汇款的媒介，这是错误的。第二，他们认为比特币等同于以往的电子汇款，这也是错误的。比特币与电子货币和电子汇款完全不同。有关比特币与电子货币的不同之处，会在第二章的第五节进行说明。

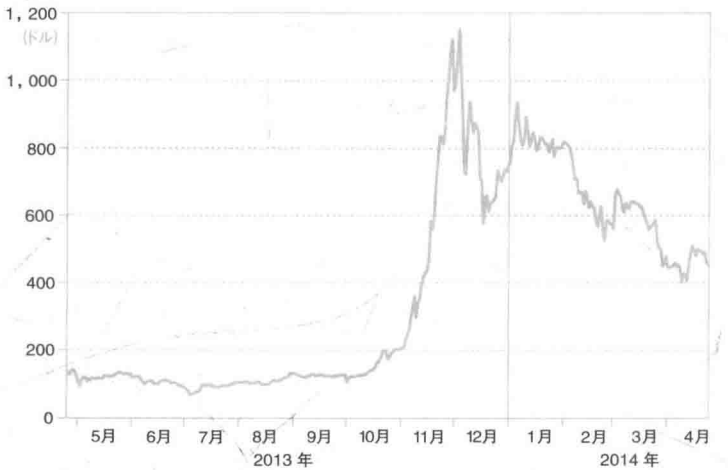
正确的情报会保护使用者

MTGOX 的破产使一些顾客无法取出比特币，有的受害者好像还持有数千万日元的比特币，这些人非常可怜。

但是，比特币是作为一种支付手段存在的，用美元或日元

进行兑换就会获得比特币，然后直接用比特币进行支付，这才是比特币正确的使用方法。而为什么这些人手中会持有比特币呢？

图表 1–1　比特币的价格变迁（单位：1BTC）



2013 年 11 月价格暴涨，后因被中国的银行禁止流通又暴跌

我们能想到的只有是投机目的。比特币在诞生后不久，因发行总额过少，与美元等现实货币的交换价值十分不稳定。2013 年 12 月初 IBTC 超过了 1000 美元，但是 12 月 18 日又回落到了 600 美元。因为中国的金融机构禁止了比特币在中国的流通，还受到了一些比 MTGOX 破产要大得多的影响。

我们回到受害顾客的问题上，在 MTGOX 公司存放数千万日元的比特币，这件事情本身似乎是一个更严重的问题。因为该公司的信用度一直都被人们所诟病。《华尔街日报》报道说：

“MTGOX 多次被黑客攻击，出现功能故障等现象”“MTGOX 的运营从一个月前就开始出现崩溃了”。

MTGOX 的破产事件，更加证明了比特币的顽强性。一个没有中央银行的货币，没有受到个别兑换所破产的影响，而继续顺畅地运营着。

当然，这并不意味着比特币不存在问题。我们已经意识到它所存在的三个问题。

第一，虽然可以追踪到比特币的交易，但却很难与现实中的个人和企业形成联系。如果将个人报酬用比特币来支付，那么税务机关就可能难以对此进行掌握，恐怕会为犯罪、洗钱等不法行为制造温床。这并非比特币的固有问题，日元本身也存在着同样的问题（但是，比特币并非完全隐匿。关于该问题参照第二章的第一节）。

第二，无法确保私人设立的兑换所以及相关服务的信用度。

第三，与美元、日元等货币的交换价值波动较大。从比特币与美元的交换比率来看，就会发现它的价值变动非常大。一般，资产的价格是由预测未来的价值所决定的。如果未来的价值总是在变动，那么资产价格也会不断地发生变化。而关于这点，现实货币也存在着同样的问题（2012 年秋到 2013 年秋，一年的时间内日元兑欧元的汇率就下跌了 50%）。另外，需要注意的一点是，在通常的商业交易中，如果收到比特币之后立即兑换为日元，就不会存在这种风险了。

重要的是我们如何处理这些问题。