1.1什么是比特币？

比特币是构成数字货币生态系统基础的概念和技术的集合。称为比特币的货币单位用于存储和传输比特币网络中的参与者之间的价值。比特币用户主要通过互联网使用比特币协议进行通信，尽管也可以使用其他传输网络。可用作开源软件的比特币协议栈可以在各种计算设备（包括笔记本电脑和智能手机）上运行，从而使该技术易于访问。

用户可以通过网络传输比特币，就像常规货币一样方便操作即可完成任何事情，包括买卖商品，汇款给别人或组织，或者扩大信用。比特币可以以专门的货币兑换方式购买，出售和兑换其他货币。比特币在某种意义上是网络的完美形式，因为它是快速，安全和无地域边界的。

与传统货币不同，比特币完全是虚拟的。没有物理硬币，甚至数字货币本身。这种币隐含在从发送方到收件人转移价值的交易中。 比特币用户有自己的密钥，允许他们证明比特币网络中的比特币的所有权。使用这些密钥，他们可以签署交易以解锁价值，并将其转移给新的所有者实现消费。钥匙通常存储在每个用户的计算机或智能手机上的数字钱包中。拥有可以签署交易的密钥是消费比特币的唯一先决条件，通过密钥实现每个用户的完全控制。

比特币是分布式的对等系统。因此，没有“中央”服务器或控制点。比特币是通过称为“挖掘”的过程创建的，该过程涉及到在处理比特币交易时竞争寻找数学问题的解决方案。比特币网络中的任何参与者（即，使用运行完整比特币协议栈的设备的任何人）可以作为矿工使用其计算机的处理能力来验证和记录交易。平均每10分钟，有人可以验证过去10分钟的交易，并获得全新的比特币奖励。基本上，比特币采矿分散了中央银行的货币发行和结算功能，取代了任何中央银行的需求。

比特币协议包括内置的算法，用于调整整个网络的采矿功能。平均而言，任何时候，无论多少矿工（以及多大处理能力）参与竞争，矿工必须执行的处理任务难度实现动态调整，保证每10分钟就可以挖矿成功。该协议还将每4年发行新比特币的比例降低一半，并将将发行的比特币的总数限制在低于2100万硬币的固定总量。结果是，流通中的比特币数量紧随其后的一个容易预测的曲线，到2140年将达到2100万。由于比特币的发行率下降，长期来看，比特币货币是通货紧缩。此外，比特币不能通过“打印”超过预期发行率的新货币来膨胀。

换句话说，比特币（bitcoin）也是协议，对等网络和分布式计算创新的代名词。比特币货币真的只是本发明的第一个应用。比特币代表了数十年密码学和分布式系统研究的高潮，包括四个关键创新，这四个创新以独特和强大的组合结合在一起。比特币这四个创新包括：去中心化的对等网络（比特币协议）公共交易总帐（区块链）独立交易确认和货币发行的一套规则（共识规则）实现有效的区块链全球去中心化共识的机制（工作量证明算法）作为一名开发人员，我将比特币视为货币互联网，通过分布式计算传播价值和确保数字资产所有权的网络。比特币还有很多比起第一眼看到的更多的内容。在本章中，我们将介绍一些主要的概念和术语，获得必要的软件，并使用比特币进行简单的交易。在接下来的章节中，我们将开始展开使比特币成为可能的技术层次，并检查比特币网络和协议的内部工作。

比特币之前的数字货币可行的数字货币的出现与密码学的发展密切相关。真正的挑战是当使用比特来代表可以交换商品和服务的价值却不以为奇。接受数字金钱的人的三个基本问题是：

我可以相信钱是真实的，不是假的吗？

我可以相信数字金钱只能花一次（被称为“双重支付”）吗？

我可以确定没有人能够声称这笔钱属于他们而不是我吗？

纸币发行商通过使用越来越复杂的纸张和印刷技术不断打击假冒问题。物理钱容易解决双重支付问题，因为同一纸币不能同时在两个地方。当然，传统的钱也经常以数字方式存储和传送。在这些情况下，假冒和双重支出问题是通过中央权威机构清算所有电子交易来处理的，中央权威机构拥有面向全球的货币视角。对于不能利用深奥油墨技术或全息条码的数字货币，密码术为信任用户对价值权利的合法性提供了依据。具体来说，加密数字签名使用户能够签署数字资产或证明该资产所有权的交易。通过适当的架构，数字签名也可用于解决双重支出问题。

当加密开始在20世纪80年代末开始变得更广泛的可用性和理解时，许多研究人员开始尝试使用加密技术构建数字货币。这些早期的数字货币项目发行数字货币，通常由国家货币或贵金属（如黄金）支持。

虽然这些早期的数字货币是有效的，但它们是集中的，因此很容易被政府和黑客攻击。早期的数字货币使用中心化的票据交易所定期进行所有交易，就像传统的银行系统一样。不幸的是，在大多数情况下，这些新兴的数字货币是政府担忧的目标，最终从法律上逐渐消失了。还有些由于当母公司突然清盘就失败了。无论是合法的政府还是犯罪分子，都需要去中心化的数字货币来避免单一的攻击避免对抗者的干预。比特币就是一种这样一个系统，通过设计实现去中心化，并且不受制于任何可能被攻击或损坏的中央权威或控制点。

1.2比特币历史

Bitcoin是在2008年由署名Satoshi Nakamoto的牛人发明的，他出版了一篇题为“Bitcoin：A Peer-to-Peer Electronic Cash System”的文章[1]。 Nakamoto结合了诸如b-money和HashCash等先前的发明，创建了一个完全去中心化的电子现金系统，它不依赖中央机构进行货币发行或结算和验证交易。关键的创新是使用分布式计算系统（称为“工作量证明”算法）每10分钟进行一次全球性的“选举”，从而允许分布式网络达成关于交易状态的共识。这优雅地解决了双重支出的问题，就是一个货币单位可以花费两次。以前，双重支出问题是数字货币的弱点，并通过中心化的票据交换所清算所有交易来解决。

比特币网络始于2009年，基于中本聪发布的参考实施指南，之后由许多其他程序员进行修订。为比特币提供安全性和弹性的工作量证明算法（挖掘）的实施以指数级增长，现在超过了世界顶级超级计算机的组合处理能力。比特币的总市值有时超过200亿美元，这取决于比特币兑美元的汇率。到目前为止，网络处理最大的交易是1.5亿美元，即时传输，无需任何费用处理。

Satoshi Nakamoto于2011年4月退出公众视线，将代码和网络的责任放在一个蓬勃发展的志愿者小组身上。比特币背后的这个人身份仍然未知。然而，中本聪和任何人都没有对比特币系统进行个人控制，这个系统基于完全透明的数学原理，开放源代码和参与者之间的共识持续运行。本发明本身具有开创性，已经延伸到分布式计算，经济学和计量经济学领域。

分布式计算问题的解决方案Satoshi Nakamoto的发明也是分布式计算当中一个古老问题的实用和新颖的解决方案，这就是 “拜占庭式将军”问题。简而言之，这个问题包括通过在不可靠和潜在的妥协网络上交换信息来尝试商定一个行动方案或一个系统的状态。 Satoshi Nakamoto的解决方案使用工作量证明的概念在没有中央信任机构的情况下实现共识，代表了分布式计算的突破，并具有超越货币的广泛适用性。可以用来达成一致的分权网络，比如彩票，资产登记，数字公证等等以证明选举的公平性。

1.3比特币使用，用户和他们的故事

比特币是古老的技术“钱”的创新。其核心在于钱方便了人与人之间的价值交流。因此，为了充分了解比特币及其用途，我们将从使用它的人的角度审视它。这里列出的每个人和他们的故事都说明了一个或多个具体的用例。我们将在整本书中看到他们：

北美低价值零售业Alice住在北加州湾区。她听她的从事技术工作的朋友说过比特币，因此想要开始使用它。我们将跟随她的故事，在她学习比特币，购买一些，然后花费一些她的比特币在帕洛阿尔托的Bob咖啡厅买一杯咖啡时。这个故事将从零售消费者的角度向我们介绍软件，交易所和基本交易。

北美高附加值零售Carol是旧金山的艺术画廊老板。她卖昂贵的绘画换取比特币。这个故事将介绍高价值物品零售商“51％”共识攻击的风险。

离岸合同服务Bob，帕洛阿尔托的咖啡店老板，正在建立一个新的网站。他与印度的网络开发商Gopesh签约，后者在印度班加罗尔居住。 Gopesh同意在比特币中支付。这个故事将研究使用比特币进行外包，合同服务和国际电汇。

网上商店Gabriel是里约热内卢的一个有进取心的年轻青少年，经营着一家小型网店，销售比特币品牌的T恤，咖啡杯和贴纸。Gabriel太年轻，没有银行账户，但他的父母鼓励他的企业精神。

慈善捐款Eugenia是菲律宾儿童慈善机构的主任。最近她已经发现了比特币，并希望利用它来接触新的国内外捐助者，为她的慈善筹款。她还在调查使用比特币快速将资金分配给需要的地区的方法。这个故事将展示使用比特币来跨币种和跨国界的全球筹款活动，以及在慈善组织中使用开放透明的分类账簿。

进出口Mohammed是迪拜的电子进口商。他正在尝试使用比特币从美国和中国购买电子产品，进口到阿联酋，以加速进口付款过程。这个故事将展示如何将比特币用于与物理商品相关的大型企业之间的国际支付。

采矿为比特币Jing是上海的计算机工程专业学生。他已经使用他的工程技术来建立一个“采矿”矿机来挖掘比特币来增加他的收入。这个故事将研究比特币的“工业”基础：用于确保比特币网络和发行新货币的专门设备。

这些故事中的每一个都是基于目前使用比特币的真实人物和实际行业，为全球经济问题创造新的市场，新的行业和创新的解决方案。

1.4入门

比特币是使用同样协议的客户端应用程序访问的协议。“比特币钱包”是比特币系统最常见的用户界面，就像Web浏览器是HTTP协议最常用的用户界面一样。有很多实施和品牌的比特币钱包，就像有许多品牌的网络浏览器（例如，Chrome，Safari，Firefox和Internet Explorer）。就像我们都有我们最喜欢的浏览器（Mozilla Firefox，Yay！）和我们不喜欢的（Internet Explorer，Yuck！），比特币钱包的质量，性能，安全性，隐私和可靠性各不相同。还有一个比特币协议的参考实现，其包括被称为“Satoshi客户端”或“比特币核心”的钱包，该钱包源于由Satoshi Nakamoto撰写的初始客户端。

1.4.1选择比特币钱包

比特币钱包是比特币生态系统中最活跃的开发的应用之一。这里竞争激烈，目前存在可能正在开发新的钱包，但也有去年的几个钱包已不再积极维护。许多钱包专注于特定的平台或具体用途，一些更适合初学者，而其他的钱包则为高级用户提供了功能。选择钱包是非常主观的，取决于使用和用户的专业知识。因此，不可能推荐一个特定的钱包品牌或项目。然而，我们可以根据其平台和功能对比特币钱包进行分类，并提供所有不同类型的钱包的一些建议。更好的是，在比特币钱包之间移动钱是容易，便宜和快速的，所以值得尝试几种不同的钱包，直到找到符合您需求的钱包。

根据平台，比特币钱包可以分类如下：

桌面钱包桌面钱包是作为参考实现创建的第一种类型的比特币钱包，许多用户运行桌面钱包以实现其功能，自主性和控制权。在通用操作系统（如Windows和Mac OS）上运行具有一定的安全隐患，因为这些平台往往不安全，配置不当。

手机钱包手机钱包是比特币钱包最常见的类型。在智能手机操作系统（如Apple iOS和Android）上运行，这些钱包通常是新用户的绝佳选择。许多都是为了简单易用而设计的，但也有功能强大的用户的全功能移动钱包。

在线钱包Web钱包通过网络浏览器访问，并将用户的钱包存储在由第三方拥有的服务器上。这类似于webmail，因为它完全依赖于第三方服务器。其中一些服务使用在用户浏览器中运行的客户端代码进行操作，该代码可以控制用户手中的比特币密钥。然而，大多数人需要在安全和方便性之间进行妥协。在第三方系统上存储大量的比特币是不合适的。

硬件钱包硬件钱包是在专用硬件上独立操作比特币钱包的设备。它们通过USB与桌面网络浏览器或通过移动设备上的近场通信（NFC）进行操作。通过专用硬件进行所有比特币相关操作，这些钱包被认为是非常安全的，适合存储大量的比特币。

纸钱包控制比特币的密钥也可以打印长期存储。即使可以使用其他材料（木材，金属等），这些也被称为纸钱包。纸钱包提供低技术但高度安全的长期存储比特币的方法。脱机存储也经常被称为冷存储。

对比特币钱包进行分类的另一种方法是通过他们的自主程度以及它们如何与比特币网络进行交互：

全节点客户端完整客户端或“完整节点”是存储比特币交易的全部历史（每个用户每次交易）的客户端，管理用户的钱包，并且可以直接在比特币网络上启动交易。完整节点处理协议的所有方面，并可以独立地验证整个区块链和任何交易。全节点客户端消耗大量计算机资源（例如，超过125 GB的磁盘，2 GB的RAM），但提供完全自主和独立的交易验证。

轻量级客户端一个轻量级的客户端，也称为简单支付验证（SPV）客户端，连接到比特币完整节点（前面提到过的），用于访问比特币交易信息，但是在本地存储用户钱包，并独立地创建，验证和传输交易。轻量级客户端与比特币网络直接交互，无需中介。

第三方API客户端第三方API客户端是通过应用程序编程接口（API）的第三方系统与比特币交互的API客户端，而不是直接连接到比特币网络。 这时钱包可能由用户或第三方服务器存储，但所有交易都需要通过第三方。

结合这些分类，比特币钱包可以分为几个小组，三个最常见的划分是桌面全客户端，移动轻巧钱包和网络第三方钱包。不同类别之间的界限通常是模糊的，许多钱包在多个平台上运行，并且可以以不同的方式与网络进行交互。

为了本书的目的，我们将演示使用各种可下载的比特币客户端，从参考实现（Bitcoin Core）到移动和网络钱包。一些示例将需要使用Bitcoin Core，除了作为完整的客户端，还可以将API暴露给钱包，网络和交易服务。如果您计划探索比特币系统中的编程接口，则需要运行Bitcoin Core或其他客户端（参见[alt_libraries]）。

1.4.2快速开始

我们在比特币使用，用户和他们的故事中介绍的Alice不是技术行家，最近只听到她的朋友Joe提到过比特币。在聚会上，Joe再次热烈地向他周围解释了比特币，并提供演示。有趣的是，Alice问她如何开始使用比特币。Joe说，手机钱包最适合新用户，他推荐了他最喜欢的几款钱包。Alice下载Android的“Mycelium”，并将其安装在手机上。

当Alice首次运行Mycelium时，与许多比特币钱包一样，应用程序会为她自动创建一个新的钱包。Alice在她的屏幕上看到钱包，如“Mycelium手机钱包”如下图1-1所示（注意：不要将比特币发送到此示例地址，它将永远丢失）。


ACCOUNTS
BALANCE
TRANSACTIONS
AD
Alice
1Cdid9KFAaat
wczBwBttQcwX
YCpvK8h7FK
0 mBTC
0.00 USD
Receive
1 BTC ~ USD 449.08 (BitcoinAverage)
Buy / Sell Bitcoin
v2.5.9

图1-1 Mycelium移动钱包

这个屏幕最重要的部分是Alice的比特币地址。 在屏幕上，它显示为一长串字母和数字：1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK。 钱包的比特币地址旁边是一个二维码，一种形式的条形码，包含可由智能相机扫描的格式的相同信息。二维码是具有黑色和白色点的图案的正方形。 Alice可以通过点击二维码或接收按钮将比特币地址或二维码复制到剪贴板上。 在大多数钱包中，点击二维码也会放大，以便更容易通过智能手机相机进行扫描。

提示比特币地址以1或3开头。像电子邮件地址一样，他们可以与其他可以使用它们的比特币用户共享，直接将比特币发送到您的钱包。 从安全角度看，关于比特币地址没有任何敏感性。 它可以在任何地方发布，而不会危及帐户的安全。 与电子邮件地址不同，您可以随意创建新的地址，所有这些都会将资金用于您的钱包。 事实上，许多现代钱包为每个交易自动创建一个新地址，以最大限度地提高隐私。 钱包只是一个地址的集合和解锁资金的钥匙。

Alice现在准备好收到资金。她的钱包应用程序随机生成一个私钥（在[private_keys]中更详细地描述）及其相应的比特币地址。在这一点上，她的比特币地址对于比特币网络来说是不知道的，或者是未经注册到比特币系统中。她的比特币地址只是一个数字，对应于一个可以用来控制资金访问的密钥。它是由她的钱包独立生成的，还没有参考或注册任何服务。事实上，在大多数钱包中，比特币地址和任何外部可识别的信息（包括用户的身份）之间没有关联。在该地址被引用作为比特币总帐的交易中的接收者之前，比特币地址只是在比特币中有效的大量可能的地址的一部分。只有一旦与交易相关联才能成为网络中已知地址的一部分。

Alice现在可以开始使用她新的比特币钱包了。

1.4.3得到你的第一个比特币

新用户的第一个也是最困难的任务是获取一些比特币。与其他外币不同，您还不能在银行或自助机购买比特币。

比特币交易是不可逆转的。大多数电子支付网络（如信用卡，借记卡，PayPal和银行帐户转帐）都是可逆的。对于销售比特币的人来说，这种差异引起了很高的风险，买方在收到比特币后会扭转电子支付，实际上欺骗了卖家。为了减轻这种风险，接受传统电子支付的公司通常要求买方进行身份验证和信用验证（可能需要几天或几周时间）。作为新用户，这意味着您不能立即使用信用卡购买比特币。需要有一点耐心和创造性的想法，但是不要着急。

以下是作为新用户得到比特币的一些方法：

找一个有比特币的朋友，直接从他或她那里买一些。许多比特币用户都是以这种方式开始的。这种方法是最不复杂的。找到比特币持有者的好办法是参加Meetup.com上列出的本地比特币会议。（在中国根本无需这么麻烦，加微信群，在线支付就可以）

使用分类服务，如localbitcoins.com来查找您所在地区的卖家，以便在现场交易中购买比特币。

通过卖比特币的产品或服务赚取比特币。如果你是程序员，出售你的编程技巧。如果你是美发师，理发只收比特币。

在你的城市使用比特币ATM。比特币自动取款机是接受现金并将比特币发送到智能手机比特币钱包的机器。使用Coin ATM Radar的在线地图找到靠近您的比特币ATM。

使用与您的银行帐户相关联的比特币货币兑换。现在有很多国家都有货币交易所，为买卖双方交易使用当地货币进行交易。实时行情服务（如BitcoinAverage）通常会显示每种货币的比特币交易所列表。

提示比特币与其他支付系统的优点之一是，当正确使用时，它为用户提供了更多的隐私。 获取，持有和支付比特币不要求您向第三方泄露敏感和个人身份信息。 但是，如果比特币涉及传统的货币交换系统，那么国家法律和国际法规就会适用。 为了兑换本币的比特币，您通常需要提供身份证明和银行信息。 用户应该知道，一旦比特币地址附加到一个身份，所有关联的比特币交易也很容易识别和跟踪。 这是许多用户选择维护专用交易账户与其钱包进行分离的一个原因。

Alice听朋友介绍比特币，所以她有一个简单的方法来获得她的第一个比特币。接下来，我们将看看她如何从她的朋友Joe 购买比特币，以Joe 如何将比特币发送到她的钱包。

1.4.4查找比特币当前价格

在Alice可以从Joe 购买比特币之前，他们必须同意比特币和美元之间的汇率。这给新兴的比特币带来了一个共同的问题："谁设定比特币价格？"简单的答案是价格是由市场设定的。

比特币与大多数其他货币一样，有浮动汇率。这意味着比特币相对于任何其他货币的价值都会根据交易的各个市场的供求情况而波动。例如，以美元计算的比特币的"价格"是根据最近的比特币和美元交易在每个市场中计算的。因此，价格往往每秒钟几次波动。定价服务将汇总来自几个市场的价格，并计算代表货币对的广泛市场汇率（例如BTC / USD）的数量加权平均数。

有数百个应用程序和网站可以提供当前的市场利率。这里有一些最受欢迎的：

Bitcoin Average一个网站，提供每种货币的体积加权平均数的简单视图。

CoinCap一项服务列出了数百种加密货币（包括比特币）的市值和汇率。

Chicago Mercantile Exchange Bitcoin Reference Rate可用于机构和合同参考的参考值，作为CME投资数据的一部分提供。

除了这些不同的网站和应用程序，大多数比特币钱包都将自动转换比特币和其他货币之间的兑换数量。 在将比特币发送给Alice之前，Joe将使用自己的钱包自动转换价格。

1.4.5发送和接收比特币

Alice决定将10美元转换成比特币，以免对这种新技术冒太多的险。她给Joe 10美元现金，打开她的Mycelium钱包应用程序，并选择Receive。这将显示一个二维码与Alice的第一个比特币地址。

Joe然后在他的智能手机钱包上选择发送，并显示一个包含两个输入的屏幕：

目的比特币地址以比特币（BTC）或其当地货币（USD）发送的金额

在比特币地址的输入字段中，有一个看起来像二维码的小图标。这样Joe可以用他的智能手机相机来扫描条形码，这样他就不必输入Alice的比特币地址，这需要非常长的时间，而且容易出错。 Joe点击二维码图标并激活智能手机相机，扫描Alice智能手机上显示的二维码。

Joe现在将Alice的比特币地址设置为收件人。Joe输入的金额为10美元，他的钱包通过访问在线服务的最新汇率来转换它。当时的汇率是每个比特币$ 100美元，所以如Joe的钱包（见图1-2Airbitz移动比特币钱包发送屏幕）截图所示，10美元的价值是0.10比特币（BTC）或100毫比银币（mBTC）。

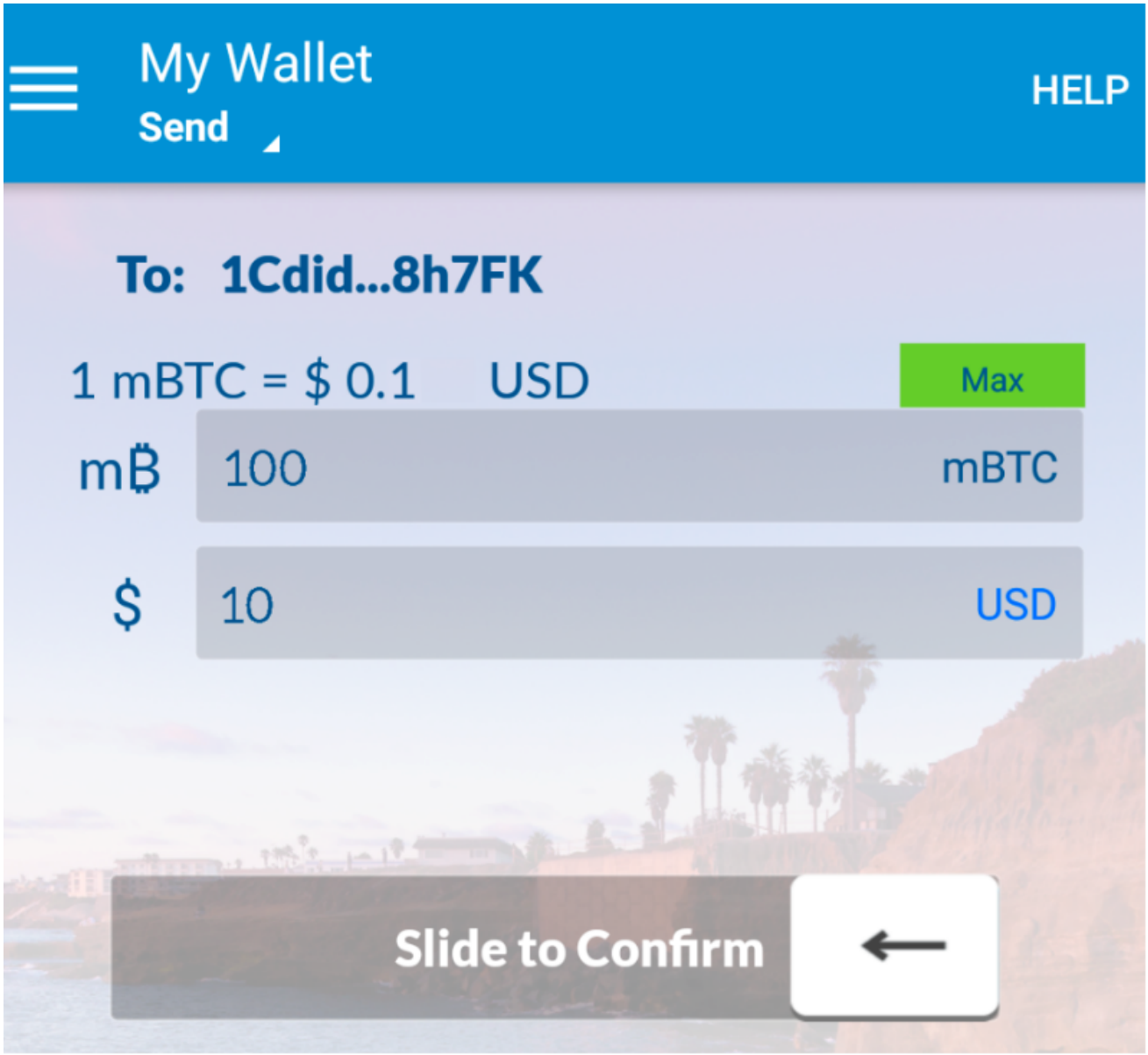

图1-2. Airbitz移动比特币钱包发送屏幕Joe然后仔细检查，以确保他已经输入了正确的金额，因为他要汇款，错误是不可逆转的。经过仔细检查地址和金额后，他按发送方式传送交易。 Joe的移动比特币钱包构建了一个交易，从Joe的钱包将0.10 BTC发送给Alice提供的地址，并用Joe的私钥签署交易。这告诉比特币网络，Joe已经授权将这笔钱转移给Alice的新地址。当交易通过对等协议传输时，它会快速传播到比特币网络。在不到一秒钟内，网络中大多数连接良好的节点都会首次接收到交易，并且首次看到Alice的地址。

同时，Alice的钱包不断地“倾听”在比特币网络上发布的交易，寻找与她的钱包中的地址匹配的任何内容。在Joe的钱包发送交易几秒钟后，Alice的钱包将显示它正在接收0.10 BTC。

确认起初，Alice的地址将把Joe的交易显示为“未确认”。这意味着交易已传播到网络，但尚未记录在比特币交易账簿即区块链中。要确认，一个交易必须包含在一个区块中，并被添加到区块链，这样的情况平均每10分钟发生一次。在传统的财务术语中，这被称为清算。有关比特币交易的传播，验证和清算（确认）的详细信息，请参阅挖矿章节[mining]。

Alice现在可以自豪地称自己是0.10 BTC的所有者了，她有权花费这些钱了。在下一章中，我们将首先用比特币进行购买，并更详细地研究底层交易和传播技术。