1介绍

1.1 What Is Bitcoin?

比特是什么?

Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called bitcoin are used to store and transmit value among participants in the bitcoin network. Bitcoin users communicate with each other using the bitcoin protocol primarily via the internet, although other transport networks can also be used. The bitcoin protocol stack, available as open source software, can be run on a wide range of computing devices, including laptops and smartphones, making the technology easily accessible.
“比特币”是一些概念和技术的集合，这些形成了“一种数字货币生态系统”的基础。
“比特币”作为货币单位，被用于在比特币网络的参与者之间的存储和转移价值。
比特币用户之间使用比特币协议进行通信，主要是通过互联网传输比特币协议，但其它传输网络也可以。
比特币协议栈是开源软件，可以运行在各种计算设备上，包括笔记本电脑和智能手机，因此使该技术易于使用。

ddk问题：概念和技术是什么意思?

Users can transfer bitcoin over the network to do just about anything that can be done with conventional currencies, including buy and sell goods, send money to people or organizations, or extend credit. Bitcoin can be purchased, sold, and exchanged for other currencies at specialized currency exchanges. Bitcoin in a sense is the perfect form of money for the internet because it is fast, secure, and borderless.
用户可以在网络上转移比特币来做任何事情，就像使用普通货币一样，包括买卖商品、汇款或提供贷款。
比特币可以以专门的货币交易所购买，出售和兑换为其它货币。
在某种意义上，比特币是互联网上货币的完美形式，因为它快速、安全、无边界。

Unlike traditional currencies, bitcoin are entirely virtual. There are no physical coins or even digital coins per se. The coins are implied in transactions that transfer value from sender to recipient. Users of bitcoin own keys that allow them to prove ownership of bitcoin in the bitcoin network. With these keys they can sign transactions to unlock the value and spend it by transferring it to a new owner. Keys are often stored in a digital wallet on each user’s computer or smartphone. Possession of the key that can sign a transaction is the only prerequisite to spending bitcoin, putting the control entirely in the hands of each user.
与传统货币不同，比特币完全是虚拟的。
没有物理货币，甚至本质上也没有数字货币。
这种货币隐含在交易中，交易将机制从付款人转移给收款人。
比特币用户有自己的密钥，允许他们证明对比特币（在比特币网络中）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来实现对它的消费。
钥匙通常存储在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条件，这使控制权完全在每个用户手中。

Bitcoin is a distributed, peer-to-peer system. As such there is no "central" server or point of control. Bitcoin are created through a process called "mining," which involves competing to find solutions to a mathematical problem while processing bitcoin transactions. Any participant in the bitcoin network (i.e., anyone using a device running the full bitcoin protocol stack) may operate as a miner, using their computer’s processing power to verify and record transactions. Every 10 minutes, on average, a bitcoin miner is able to validate

the transactions of the past 10 minutes and is rewarded with brand new bitcoin. Essentially, bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank and replaces the need for any central bank.
比特币是分布式的P2P系统。因此，没有“中央”服务器或控制点。
通过“挖矿”过程创造比特币，“挖矿”是在处理比特币交易时，竞争寻找一个数学题的解。
比特币网络中的任何参与者（即，任何运行全比特币协议栈的设备）都可以是矿工，它们使用计算机的处理能力来验证和记录交易。平均每10分钟，一个比特币矿工能够批准过去10分钟的交易，并获得新比特币奖励。
本质上，比特币挖矿使“中央银行的货币发行和计算功能”去中心化了，从而取代了中央银行。

The bitcoin protocol includes built-in algorithms that regulate the mining function across the network. The difficulty of the processing task that miners must perform is adjusted dynamically so that, on average, someone succeeds every 10 minutes regardless of how many miners (and how much processing) are competing at any moment. The protocol also halves the rate at which new bitcoin are created every 4 years, and limits the total number of bitcoin that will be created to a fixed total just below 21 million coins. The result is that the number of bitcoin in circulation closely follows an easily predictable curve that approaches 21 million by the year 2140. Due to bitcoin's diminishing rate of issuance, over the long term, the bitcoin currency is deflationary. Furthermore, bitcoin cannot be inflated by "printing" new money above and beyond the expected issuance rate.
“比特币协议”包括了内置的算法，可以在网络中调整挖矿工作。
矿工们要执行的处理任务的难度是动态调整的，因此，平均而言，每10分钟就有一个人能成功，而不管那时有多少矿工和多少处理能力在竞争。
这个协议还规定，每隔4年，发行的新比特币被减半，这将比特币的总量限制为低于2100万。
结果是，流通中的比特币数量遵循一个容易预测的曲线，到2140年将达到2100万。
由于比特币发行速率的下降，长期来看，比特币是通货紧缩。
此外，无法通过这种方法使比特币通胀：以超过预期发行速率来“印刷”新钱。

Behind the scenes, bitcoin is also the name of the protocol, a peer-to-peer network, and a distributed computing innovation. The bitcoin currency is really only the first application of this invention. Bitcoin represents the culmination of decades of research in cryptography and distributed systems and includes four key innovations brought together in a unique and powerful combination.
在幕后，比特币（bitcoin）也代表：这种协议、一种P2P网络、一种分布式计算创新。
“比特币货币”只是这个发明的第一个应用。
比特币代表了数十年来在密码学和分布式系统领域研究的高潮，它包括四个主要创新，形成了一个独特和强大的组合。

Bitcoin consists of:
- A decentralized peer-to-peer network (the bitcoin protocol)
- A public transaction ledger (the blockchain)
- A set of rules for independent transaction validation and currency issuance (consensus rules)
- A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm)

比特币包括：
- 一个去中心化的P2P网络 （比特币协议）
- 一个公共交易账本 （区块链）
- 一套规则，用于独立的交易确认和货币发行 （共识规则）
- 一个机制，用于对有效区块链实现全球去中性化共识 （工作量证明算法）

ddk问题：这四个部分怎么构成比特币？为什么是这四个？

As a developer, I see bitcoin as akin to the internet of money, a network for propagating value and securing the ownership of digital assets via distributed computation. There's a lot more to bitcoin than first meets the eye.
作为一名开发人员，我认为比特币类似于货币互联网，它是一个网络，通过分布式计算来转播价值和保证数字资产的所有权。

比特币的内容比初看时要多得多。

In this chapter we'll get started by explaining some of the main concepts and terms, getting the necessary software, and using bitcoin for simple transactions. In following chapters we'll start unwrapping the layers of technology that make bitcoin possible and examine the inner workings of the bitcoin network and protocol.
在本章中，我们先解释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。
在后面章节中，我们将展开使比特币成为可能的技术层次，并考察比特币网络和协议的内部工作。

Digital Currencies Before Bitcoin
比特币之前的数字货币

The emergence of viable digital money is closely linked to developments in cryptography. This is not surprising when one considers the fundamental challenges involved with using bits to represent value that can be exchanged for goods and services. Three basic questions for anyone accepting digital money are:
1. Can I trust that the money is authentic and not counterfeit?
2. Can I trust that the digital money can only be spent once (known as the "double-spend" problem)?
3. Can I be sure that no one else can claim this money belongs to them and not me?

可行的数字货币的出现与密码学的发展密切相关。
这并不奇怪，因为人们要考虑面临的主要挑战：使用比特来表示价值，并且能用于交换商品和服务。
任何接受数字货币的人，都要面对三个基本问题：

- 我能否相信这些货币是真实的，不是伪造的? 真钱
- 我能否相信这些数字货币只能花费一次? 不能双重支付
- 我能否确认没有其他人能声称这些钱属于他们？只属于我

Issuers of paper money are constantly battling the counterfeiting problem by using increasingly sophisticated papers and printing technology. Physical money addresses the double-spend issue easily because the same paper note cannot be in two places at once. Of course, conventional money is also often stored and transmitted digitally. In these cases, the counterfeiting and double-spend issues are handled by clearing all electronic transactions through central authorities that have a global view of the currency in circulation.
纸币的发行者通过使用复杂的纸张和印刷技术不断打击假冒问题。
物理货币很容易解决双重支付问题，因为同一货币不会同时在两个地方。
当然，传统货币也经常以数字方式存储和转移。
在这些情况下，假冒和双重支出问题是通过中央权威机构来解决：它有流通货币的全局视图，它来清算所有电子交易。

For digital money, which cannot take advantage of esoteric inks or holographic strips, cryptography provides the basis for trusting the legitimacy of a user's claim to value. Specifically, cryptographic digital signatures enable a user to sign a digital asset or transaction proving the ownership of that asset. With the appropriate architecture, digital signatures also can be used to address the double-spend issue.
数字货币没法利用油墨技术或全息条码，而密码学为信任用户的价值主张的合法性提供了基础。
具体来说，加密数字签名能使用户对数字资产或交易进行签名，以证明对该资产所有权。
使用适当的体系结构，数字签名还能用于解决双重支付问题。

When cryptography started becoming more broadly available and understood in the late 1980s, many researchers began trying to use cryptography to build digital currencies. These early digital currency projects issued digital money, usually backed by a national currency or precious metal such as gold.
当密码学1980年代后期开始变得更广泛得可用和被理解时，许多研究人员开始尝试使用密码学来构建数字货币。
这些早期的数字货币项目发行了数字货币，通常有国家货币或贵金属（如黄金）支持。

Although these earlier digital currencies worked, they were centralized and, as a result, were easy to attack by governments and hackers. Early digital currencies used a central

clearinghouse to settle all transactions at regular intervals, just like a traditional banking system. Unfortunately, in most cases these nascent digital currencies were targeted by worried governments and eventually litigated out of existence. Some failed in spectacular crashes when the parent company liquidated abruptly. To be robust against intervention by antagonists, whether legitimate governments or criminal elements, a *decentralized* digital currency was needed to avoid a single point of attack. Bitcoin is such a system, decentralized by design, and free of any central authority or point of control that can be attacked or corrupted.

虽然这些早期的数字货币可以用，但它们是集中式的，因此，很容易受到政府和黑客的攻击。

早期的数字货币使用中心化的票据交易所定期清算所有交易，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被忧心忡忡的政府所瞄准，最终被剥夺了生存权。

有些是由于母公司突然破产，导致在巨大崩溃中失败。

为了在对手干扰的情况下保持稳定性，无论是合法政府还是犯罪分子，都需要一个去中心化的数字货币，以避免单点攻击。

比特币就是这样一个系统，它被设计为区去中性化，并免受任何中央权威或控制点被攻击或破坏。

1.2比特币历史

Bitcoin was invented in 2008 with the publication of a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System,"[1] written under the alias of Satoshi Nakamoto (see [satoshi_whitepaper]).
比特币发明于2008年，当时署名Satoshi Nakamoto（中本聪）的人发表了一篇题文章：
Bitcoin: A Peer-to-Peer Electronic Cash System

Nakamoto combined several prior inventions such as b-money and HashCash to create a completely decentralized electronic cash system that does not rely on a central authority for currency issuance or settlement and validation of transactions. The key innovation was to use a distributed computation system (called a "Proof-of-Work" algorithm) to conduct a global "election" every 10 minutes, allowing the decentralized network to arrive at *consensus* about the state of transactions. This elegantly solves the issue of double-spend where a single currency unit can be spent twice. Previously, the double-spend problem was a weakness of digital currency and was addressed by clearing all transactions through a central clearinghouse.
中本聪综合了多个以前的发明，例如b-money和HashCash，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交易结算和验证。
主要的创新是使用了一个分布式计算系统（称为“工作量证明”算法），它每10分钟进行一次全球“选举”，从而允许这个去中性化网络对交易的状态达成共识。
这优雅地解决了双重支付问题，就是一个货币单位被花费两次。
以前，双重支付问题是数字货币的弱点，是通过一个中心票据交易所清算所有交易来解决。

The bitcoin network started in 2009, based on a reference implementation published by Nakamoto and since revised by many other programmers. The implementation of the Proof-of-Work algorithm (mining) that provides security and resilience for bitcoin has increased in power exponentially, and now exceeds the combined processing power of the world's top supercomputers. Bitcoin's total market value has at times exceeded $135 billion US dollars, depending on the bitcoin-to-dollar exchange rate. The largest transaction processed so far by the network was $400 million US dollars, transmitted instantly and processed for a fee of $1.
比特币网络始于2009年，它是基于中本聪发布的一个参考实现，之后由许多其他程序员做了修改。
工作量证明算法（挖矿）为比特币提供了安全性和弹性，它的实现以指数级增长，现在已超过了世界顶级超级计算机的综合处理能力。
比特币的总市值有时超过135亿美元，这取决于比特币与美元的汇率。
到目前为止，网络处理最大的交易是400万美元，它被立即发送和处理，费用只有1美元。

Satoshi Nakamoto withdrew from the public in April 2011, leaving the responsibility of developing the code and network to a thriving group of volunteers. The identity of the person or people behind bitcoin is still unknown. However, neither Satoshi Nakamoto nor anyone else exerts individual control over the bitcoin system, which operates based on fully transparent mathematical principles, open source code, and consensus among participants. The invention itself is groundbreaking and has already spawned new science in the fields of distributed computing, economics, and econometrics.
中本聪于2011年4月退出公众视线，将开发代码和网络的责任留给了一个蓬勃发展的志愿者小组。
中本聪的身份仍然未知。然而，无论是中本聪还是其他人，都没法单独控制比特币系统，这个系统的运作是基于完全透明的数学原理、开放的源代码、参与者之间的共识。
这项发明本身具有开创性，已经在分布式计算、经济学和计量经济学领域催生了新的科学。

A Solution to a Distributed Computing Problem
分布式计算问题的解决方案

Satoshi Nakamoto's invention is also a practical and novel solution to a problem in distributed computing, known as the "Byzantine Generals' Problem." Briefly, the problem consists of trying to agree on a course of action or the state of a system by exchanging information over an unreliable and potentially compromised network.

中本聪的发明也是对分布式计算中一个问题的实用和新颖的解决方案，这就是 “拜占庭式将军问题”。
简单地说，这个问题是：试图通过一个不可靠和易受攻击的网络上，对行动方案或系统状态达成一致意见。

Satoshi Nakamoto’s solution, which uses the concept of Proof-of-Work to achieve consensus *without a central trusted authority*, represents a breakthrough in distributed computing and has wide applicability beyond currency. It can be used to achieve consensus on decentralized networks to prove the fairness of elections, lotteries, asset registries, digital notarization, and more.
中本聪的解决方案使用了工作量证明的概念，在没有中央信任机构的情况下实现了共识，这个方案代表了分布式计算上的突破，并在货币之外有广泛的适用性。
它可用来在去中性化网络上达成共识，以证明下列的公平性：选举、博彩、资产登记、数字公证、等等。

1.3比特币的使用、用户和他们的故事

Bitcoin is an innovation in the ancient technology of money. At its core, money simply facilitates the exchange of value between people. Therefore, in order to fully understand bitcoin and its uses, we'll examine it from the perspective of people using it. Each of the people and their stories, as listed here, illustrates one or more specific use cases. We'll be seeing them throughout the book:
比特币是对古老的钱币技术的创新。
在其核心，钱只是方便人们之间交换价值。
因此，为了充分理解比特币及其用途，我们将从使用者的角度来审视它。
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。

（1）North American low-value retail　北美低价值的零售
Alice lives in Northern California's Bay Area. She has heard about bitcoin from her techie friends and wants to start using it. We will follow her story as she learns about bitcoin, acquires some, and then spends some of her bitcoin to buy a cup of coffee at Bob's Cafe in Palo Alto. This story will introduce us to the software, the exchanges, and basic transactions from the perspective of a retail consumer.
Alice住在北部加州的湾区。她从搞技术工作的朋友那里听说过比特币，因此想要使用它。
她要了解比特币，获得一些比特币，然后花费一些比特币从Bob的咖啡店买一杯咖啡。
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。

（2）North American high-value retail　北美高价值的零售
Carol is an art gallery owner in San Francisco. She sells expensive paintings for bitcoin. This story will introduce the risks of a "51%" consensus attack for retailers of high-value items.
Carol是旧金山的艺术画廊老板。她卖昂贵的油画换取比特币。
这个故事将介绍，对于高价值商品的零售商来说，有"51%共识攻击"的风险。

（3）Offshore contract services　国外合约服务
Bob, the cafe owner in Palo Alto, is building a new website. He has contracted with an Indian web developer, Gopesh, who lives in Bangalore, India. Gopesh has agreed to be paid in bitcoin. This story will examine the use of bitcoin for outsourcing, contract services, and international wire transfers.
Bob是咖啡店的老板，正在建一个新的网站。
他联系了一个印度的Web开发者（Gopesh），Gopesh住在印度班加罗尔。
Gopesh同意Bob向他支付比特币。
这个故事将研究比特币用于：外包、合约服务、国际电汇。

（4）Web store　Web商店
Gabriel is an enterprising young teenager in Rio de Janeiro, running a small web store that sells bitcoin-branded t-shirts, coffee mugs, and stickers. Gabriel is too young to have a bank account, but his parents are encouraging his entrepreneurial spirit.
Gabriel是里约热内卢的一个有进取心的青少年，经营着一个小网店，销售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创业精神。

（5）Charitable donations　慈善捐款
Eugenia is the director of a children's charity in the Philippines. Recently she has discovered bitcoin and wants to use it to reach a whole new group of foreign and domestic donors to fundraise for her charity. She's also investigating ways to use bitcoin to distribute funds quickly to areas of need. This story will show the use of bitcoin for global fundraising across currencies and borders and the use of an open ledger for transparency in charitable organizations.
Eugenia是菲律宾儿童慈善机构的主管。
最近她发现了比特币，想利用它来让一个新的外国和国内捐助团体为她的慈善事业募捐。

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。
这个故事将展示了使用比特币来进行跨币种和跨国界的全球筹款活动，并在慈善组织中使用透明的开放账本。

（6）Import/export　进出口

Mohammed is an electronics importer in Dubai. He's trying to use bitcoin to buy electronics from the United States and China for import into the UAE to accelerate the process of payments for imports. This story will show how bitcoin can be used for large business-to-business international payments tied to physical goods.
Mohammed是迪拜的一个电子进口商。
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。

（7）Mining for bitcoin　比特币挖矿

Jing is a computer engineering student in Shanghai. He has built a "mining" rig to mine for bitcoin using his engineering skills to supplement his income. This story will examine the "industrial" base of bitcoin: the specialized equipment used to secure the bitcoin network and issue new currency.
Jing是上海的一名计算机专业的学生。
他已经使用他的技术技能建立一个“挖矿”矿机，来挖掘比特币，来补充他的收入。
这个故事将研究比特币的“产业”基础：专门的设备用于保证比特币网络的安全和发行新货币。

Each of these stories is based on the real people and real industries currently using bitcoin to create new markets, new industries, and innovative solutions to global economic issues.
这些故事都是基于真实的人和真实的行业，他们使用比特币为创建了新的市场、新的行业，为全球经济问题提供了创新的解决方案。

1.4入门

Bitcoin is a protocol that can be accessed using a client application that speaks the protocol. A "bitcoin wallet" is the most common user interface to the bitcoin system, just like a web browser is the most common user interface for the HTTP protocol. There are many implementations and brands of bitcoin wallets, just like there are many brands of web browsers (e.g., Chrome, Safari, Firefox, and Internet Explorer). And just like we all have our favorite browsers (Mozilla Firefox, Yay!) and our villains (Internet Explorer, Yuck!), bitcoin wallets vary in quality, performance, security, privacy, and reliability. There is also a reference implementation of the bitcoin protocol that includes a wallet, known as the "Satoshi Client" or "Bitcoin Core," which is derived from the original implementation written by Satoshi Nakamoto.
比特币是一个协议，可以使用讲这个协议的客户端应用程序来访问它。
“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协议最常见的用户界面一样。
比特币钱包有很多实现和品牌，就像有许多Web浏览器一样（例如Chrome、Safari、Firefox和IE）。
就像我们都有自己喜欢的浏览器和不喜欢的浏览器，比特币钱包的质量、性能、安全性、隐私和可靠性也各不相同。
还有比特币协议的一个参考实现，它包含一个钱包，称为“中本聪客户端”或“Bitcoin Core”，它源于中本聪编写的最初实现。

1.4.1选择一个比特币钱包

Bitcoin wallets are one of the most actively developed applications in the bitcoin ecosystem. There is intense competition, and while a new wallet is probably being developed right now, several wallets from last year are no longer actively maintained.
“比特币钱包”是“比特币生态系统”中最积极开发的应用之一。
这里竞争激烈，虽然一个新的钱包现在可能正在开发，但去年的一些钱包可能不再被积极维护。

Many wallets focus on specific platforms or specific uses and some are more suitable for beginners while others are filled with features for advanced users. Choosing a wallet is highly subjective and depends on the use and user expertise. It is therefore impossible to recommend a specific brand or wallet. However, we can categorize bitcoin wallets according to their platform and function and provide some clarity about all the different types of wallets that exist. Better yet, moving keys or seeds between bitcoin wallets is relatively easy, so it is worth trying out several different wallets until you find one that fits your needs.
许多钱包专注于特定的平台或具体用途，一些更适合新手，而其它钱包则为高级用户提供了许多功能。
选择钱包是非常主观的，取决于用途和用户的专业知识。因此，不可能推荐一个特定的品牌或钱包。
然而，我们可以根据平台和功能对比特币钱包进行分类，并使不同类型的钱包更加清晰。
比较好的是，在比特币钱包之间移动密钥和种子（seed）相对比较容易，所以可以尝试几种不同的钱包，找到符合你需求的钱包。

Bitcoin wallets can be categorized as follows, according to the platform:
根据平台，比特币钱包做如下分类。

（1）Desktop wallet　桌面钱包
A desktop wallet was the first type of bitcoin wallet created as a reference implementation and many users run desktop wallets for the features, autonomy, and control they offer. Running on general-use operating systems such as Windows and Mac OS has certain security disadvantages however, as these platforms are often insecure and poorly configured.

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，因为它提供了功能、自主权和控制。
但是，在通用操作系统（如Windows和Mac OS）上运行桌面钱包有一定的安全隐患，因为这些平台往往不安全，并且配置不当。

（2）Mobile wallet 手机钱包

A mobile wallet is the most common type of bitcoin wallet. Running on smart-phone operating systems such as Apple iOS and Android, these wallets are often a great choice for new users. Many are designed for simplicity and ease-of-use, but there are also fully featured mobile wallets for power users.
手机钱包是最常用的比特币钱包。
在智能手机操作系统（如iOS和Android）上运行，这些钱包通常是新用户的绝佳选择。
许多都设计为简单易用，但也有全功能移动钱包。

（3）Web wallet Web钱包

Web wallets are accessed through a web browser and store the user's wallet on a server owned by a third party. This is similar to webmail in that it relies entirely on a third-party server. Some of these services operate using client-side code running in the user's browser, which keeps control of the bitcoin keys in the hands of the user. Most, however, present a compromise by taking control of the bitcoin keys from users in exchange for ease-of-use. It is inadvisable to store large amounts of bitcoin on third-party systems.
Web钱包通过Web浏览器访问，将用户的钱包存储在由第三方的服务器上。
这类似于webmail，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，这使比特币密钥控制在用户手里。
但是，多数提供的是一个折衷方案，即从用户手中获取对比特币密钥的控制，从而换取方便使用。
把大量比特币存在第三方系统上是不合适的。

（4）Hardware wallet 硬件钱包

Hardware wallets are devices that operate a secure self-contained bitcoin wallet on special-purpose hardware. They are operated via USB with a desktop web browser or via near-field-communication (NFC) on a mobile device. By handling all bitcoin-related operations on the specialized hardware, these wallets are considered very secure and suitable for storing large amounts of bitcoin.
硬件钱包是某种设备，它在专用硬件上操作一个安全的独立的比特币钱包。
使用一个桌面Web浏览器通过USB来操作它们，或者在移动设备上通过NFC来操作它们。
通过在专用硬件上处理所有比特币相关操作，这些钱包被认为非常安全，适合存储大量的比特币。

（5）Paper wallet 纸钱包

The keys controlling bitcoin can also be printed for long-term storage. These are known as paper wallets even though other materials (wood, metal, etc.) can be used. Paper wallets offer a low-tech but highly secure means of storing bitcoin long term. Offline storage is also often referred to as *cold storage*.
控制比特币的密钥也可以打印下来，用于长期存储。
这些被称为纸钱包，即使使用的是其它材料（木头、金属等）。
纸钱包使用的是低技术，但提供了长期存储比特币的高度安全的方法。
“离线存储”也经常被称为“冷存储”。

Another way to categorize bitcoin wallets is by their degree of autonomy and how they interact with the bitcoin network:
对比特币钱包的另一种分类方法是，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。

（1）Full-node client 全节点客户端

A full client, or "full node," is a client that stores the entire history of bitcoin transactions (every transaction by every user, ever), manages users' wallets, and can initiate transactions directly on the bitcoin network. A full node handles all aspects of the protocol and can independently validate the entire blockchain and any transaction. A full-node client consumes substantial computer resources (e.g., more than 125 GB of disk, 2 GB of RAM) but offers complete autonomy and independent transaction verification.

全客户端（全节点）存储比特币交易的全部历史（每个用户的每个交易），管理用户的钱包，并且可以直接在比特币网络上发起交易。
全节点处理协议的所有方面，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，至少125 GB磁盘，2 GB RAM），但它提供完全自主和独立的交易验证。

（2）Lightweight client 轻量级客户端
A lightweight client, also known as a simple-payment-verification (SPV) client, connects to bitcoin full nodes (mentioned previously) for access to the bitcoin transaction information, but stores the user wallet locally and independently creates, validates, and transmits transactions. Lightweight clients interact directly with the bitcoin network, without an intermediary.
轻量级的客户端（SPV）连接到比特币全节点，以便获得比特币交易信息，但是在本地存储用户钱包，并独立地创建、验证和发送交易。
轻量级客户端直接与比特币网络交互，没有中介。

（3）Third-party API client 第三方API客户端
A third-party API client is one that interacts with bitcoin through a third-party system of application programming interfaces (APIs), rather than by connecting to the bitcoin network directly. The wallet may be stored by the user or by third-party servers, but all transactions go through a third party.
“第三方API客户端”通过第三方系统API与比特币进行交互，它不是直接连接到比特币网络。
钱包可能由用户或第三方服务器存储，但所有交易都要经过第三方。

Combining these categorizations, many bitcoin wallets fall into a few groups, with the three most common being desktop full client, mobile lightweight wallet, and web third-party wallet. The lines between different categories are often blurry, as many wallets run on multiple platforms and can interact with the network in different ways.
综合这些分类，许多比特币钱包可以归为几个组，三个最常见的划分是：
桌面全客户端、移动轻量级钱包、Web第三方钱包。
不同类别之间的界限通常是模糊的，因为许多钱包在多个平台上运行，并且能以不同的方式与网络进行交互。

For the purposes of this book, we will be demonstrating the use of a variety of downloadable bitcoin clients, from the reference implementation (Bitcoin Core) to mobile and web wallets. Some of the examples will require the use of Bitcoin Core, which, in addition to being a full client, also exposes APIs to the wallet, network, and transaction services. If you are planning to explore the programmatic interfaces into the bitcoin system, you will need to run Bitcoin Core, or one of the alternative clients (see [alt_libraries]).
在本书中，将演示各种可下载的比特币客户端的使用，从参考实现（Bitcoin Core）到移动和Web钱包。
一些例子要使用Bitcoin Core，除了作为一个全客户端，还给钱包、网络和交易服务提供API。
如果你要探索比特币系统中的编程接口，则需要运行Bitcoin Core或其它客户端（参见[alt_libraries]）。

1.4.2快速开始

Alice, who we introduced in Bitcoin Uses, Users, and Their Stories, is not a technical user and only recently heard about bitcoin from her friend Joe. While at a party, Joe is once again enthusiastically explaining bitcoin to all around him and is offering a demonstration. Intrigued, Alice asks how she can get started with bitcoin. Joe says that a mobile wallet is best for new users and he recommends a few of his favorite wallets. Alice downloads "Mycelium" for Android and installs it on her phone.
在1.3节提到，Alice不是技术行家，最近听到她的朋友Joe提到过比特币。
在聚会上，Joe再次热烈地向周围的人介绍比特币，并做了演示。

Alice很好骑，问他如何开始使用比特币。
Joe说，手机钱包最适合新用户，并推荐了他最喜欢的几款钱包。
Alice在Android上下载了“Mycelium”，并安装到手机上。

When Alice runs Mycelium for the first time, as with many bitcoin wallets, the application automatically creates a new wallet for her. Alice sees the wallet on her screen, as shown in The Mycelium Mobile Wallet (note: do *not* send bitcoin to this sample address, it will be lost forever).
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在屏幕上看到了这个钱包，如下图1-1所示。

Figure 1. The Mycelium Mobile Wallet
图1-1 Mycelium手机钱包

The most important part of this screen is Alice's *bitcoin address*. On the screen it appears as a long string of letters and numbers: 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK. Next to the wallet's bitcoin address is a QR code, a form of barcode that contains the same information in a format that can be scanned by a smartphone camera. The QR code is the square with a pattern of black and white dots. Alice can copy the bitcoin address or the QR code onto her clipboard by tapping the QR code, or the Receive button. In most wallets, tapping the QR code will also magnify it, so that it can be more easily scanned by a smartphone camera.
在这个屏幕中，最重要的部分是Alice的比特币地址。
在屏幕上，它显示为一个字符串：1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
比特币地址旁边是一个二维码，它包含相同的信息。
Alice可以通过点击二维码或Receive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，点击二维码会将其放大，以便更容易使用手机进行扫描。

Tip: Bitcoin addresses start with a 1 or 3. Like email addresses, they can be shared with other bitcoin users who can use them to send bitcoin directly to your wallet. There is nothing sensitive, from a security perspective, about the bitcoin address. It can be posted anywhere without risking the security of the account. Unlike email addresses, you can create new addresses as often as you like, all of which will direct funds to your wallet. In fact, many modern wallets automatically create a new address for every transaction

to maximize privacy. A wallet is simply a collection of addresses and the keys that unlock the funds within.
提示：比特币地址以1或3开头。
与email地址一样，可以把比特币地址共享给其他比特币用户，这些用户可以直接用比特币地址向你的钱包发送比特币。
从安全角度看，比特币地址没有任何敏感性。它可以发布在任何地方，不会危及帐户的安全。
与email地址不同的是，你可以随意创建新的比特币地址，所有这些地址都会将资金导入到你的钱包。
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。
钱包只是一些地址和密钥的集合，密钥用于解锁钱包中的资金。

Alice is now ready to receive funds. Her wallet application randomly generated a private key (described in more detail in [private_keys]) together with its corresponding bitcoin address. At this point, her bitcoin address is not known to the bitcoin network or "registered" with any part of the bitcoin system. Her bitcoin address is simply a number that corresponds to a key that she can use to control access to the funds. It was generated independently by her wallet without reference or registration with any service. In fact, in most wallets, there is no association between the bitcoin address and any externally identifiable information including the user's identity. Until the moment this address is referenced as the recipient of value in a transaction posted on the bitcoin ledger, the bitcoin address is simply part of the vast number of possible addresses that are valid in bitcoin. Only once it has been associated with a transaction does it become part of the known addresses in the network.
Alice现在准备收取资金。
她的钱包应用程序随机生成一个私钥和对应的比特币地址。
此时，比特币网络还不知道她的比特币地址，也没有注册到比特币系统的任何地方。
她的比特币地址只是一个数字，对应一个密钥，可以用这个密钥控制资金的访问。
它是由钱包独立生成的，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。
在该地址被用作为比特币账目上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。只有当它与交易关联时，它才成为网络中已知地址的一部分。

Alice is now ready to start using her new bitcoin wallet.
Alice现在可以开始使用她的新比特币钱包了。

1.4.3获得第一个比特币

The first and often most difficult task for new users is to acquire some bitcoin. Unlike other foreign currencies, you cannot yet buy bitcoin at a bank or foreign exchange kiosk.
新用户的第一个，也是最困难的任务是获取一些比特币。
与其它外币不同，你还不能在银行或自助机上购买比特币。

Bitcoin transactions are irreversible. Most electronic payment networks such as credit cards, debit cards, PayPal, and bank account transfers are reversible. For someone selling bitcoin, this difference introduces a very high risk that the buyer will reverse the electronic payment after they have received bitcoin, in effect defrauding the seller. To mitigate this risk, companies accepting traditional electronic payments in return for bitcoin usually require buyers to undergo identity verification and credit-worthiness checks, which may take several days or weeks. As a new user, this means you cannot buy bitcoin instantly with a credit card. With a bit of patience and creative thinking, however, you won't need to.
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。
对于卖比特币的人来说，这种差异引起了很高的风险：买方在收到比特币后，会逆转电子支付，实际上是欺骗了卖家。
为了降低这种风险，接受传统电子支付作为比特币的回报的公司通常要求购买者进行身份验证和资信检查，这可能需要几天或几周的时间。

作为新用户，这意味着你不能立即使用信用卡购买比特币。然而，只要有一点耐心和创造性的思考，你就不需要了。

ddk问题：传统支付有欺诈风险，比特币的这方面风险更低，那么传统支付是怎么实现欺诈的呢?

Here are some methods for getting bitcoin as a new user:
以下是新用户得到比特币的一些方法：

- Find a friend who has bitcoin and buy some from him or her directly. Many bitcoin users start this way. This method is the least complicated. One way to meet people with bitcoin is to attend a local bitcoin meetup listed at Meetup.com.
  找一个有比特币的朋友，直接从他那里买一些。许多比特币用户都是以这种方式开始的。
  这种方法最简单。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。

- Use a classified service such as localbitcoins.com to find a seller in your area to buy bitcoin for cash in an in-person transaction.
  使用一个分类服务，如localbitcoins.com，来查找你所在地区的卖家，以便在现场交易中购买比特币。

- Earn bitcoin by selling a product or service for bitcoin. If you are a programmer, sell your programming skills. If you're a hairdresser, cut hair for bitcoin.

  通过卖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。

- Use a bitcoin ATM in your city. A bitcoin ATM is a machine that accepts cash and sends bitcoin to your smartphone bitcoin wallet. Find a bitcoin ATM close to you using an online map from Coin ATM Radar.
  在你的城市使用比特币ATM。比特币ATM是接受现金并将比特币发送到手机比特币钱包的机器。
  使用Coin ATM Radar的在线地图找到离你最近的比特币ATM。

- Use a bitcoin currency exchange linked to your bank account. Many countries now have currency exchanges that offer a market for buyers and sellers to swap bitcoin with local currency. Exchange-rate listing services, such as BitcoinAverage, often show a list of bitcoin exchanges for each currency.

  使用链接到你的银行账户的一个比特币货币交易所。
  现在有很多国家都有货币交易所，为买卖双方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。

Tip: One of the advantages of bitcoin over other payment systems is that, when used correctly, it affords users much more privacy. Acquiring, holding, and spending bitcoin does not require you to divulge sensitive and personally identifiable information to third parties. However, where bitcoin touches traditional systems, such as currency exchanges, national and international regulations often apply. In order to exchange bitcoin for your national currency, you will often be required to provide proof of identity and banking information. Users should be aware that once a bitcoin address is attached to an identity, all associated bitcoin transactions are also easy to identify and track. This is one reason many users choose to maintain dedicated exchange accounts unlinked to their wallets.
提示：
比特币相比其它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你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。
为了把比特币兑换成本国货币，你通常需要提供身份证明和银行信息。
用户应该意识到，一旦比特币地址与一个身份关联，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换账户（与其钱包没有关联）的一个原因。

Alice was introduced to bitcoin by a friend so she has an easy way to acquire her first bitcoin. Next, we will look at how she buys bitcoin from her friend Joe and how Joe sends the bitcoin to her wallet.
Alice听了朋友介绍比特币，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，我们看看她如何从Joe 那里购买比特币，以及Joe 如何将比特币发送到她的钱包。

1.4.4查询比特币当前价格

Before Alice can buy bitcoin from Joe, they have to agree on the *exchange rate* between bitcoin and US dollars. This brings up a common question for those new to bitcoin: "Who sets the bitcoin price?" The short answer is that the price is set by markets.
在Alice从Joe 购买比特币之前，他们必须协商比特币和美元之间的汇率。
这给新兴的比特币带来了一个常见的问题：谁设定了比特币的价格?
简单的答案是：价格是由市场设定的。

Bitcoin, like most other currencies, has a *floating exchange rate*. That means that the value of bitcoin vis-a-vis any other currency fluctuates according to supply and demand in the various markets where it is traded. For example, the "price" of bitcoin in US dollars is calculated in each market based on the most recent trade of bitcoin and US dollars. As such, the price tends to fluctuate minutely several times per second. A pricing service will aggregate the prices from several markets and calculate a volume-weighted average representing the broad market exchange rate of a currency pair (e.g., BTC/USD).
比特币与大多数其他货币一样，有一个浮动汇率。
这意味着，比特币相对于任何其它货币的价值都会根据交易的各种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，并计算一个加权平均值，它代表了“货币对”（例如BTC/USD）的广泛市场汇率。

There are hundreds of applications and websites that can provide the current market rate. Here are some of the most popular:
有几百个应用程序和网站，可以提供当前的市场汇率。这里有一些最受欢迎的。

Bitcoin Average
A site that provides a simple view of the volume-weighted-average for each currency.

Bitcoin Average：一个网站，提供了每种货币的加权平均值的简单视图。

CoinCap
A service listing the market capitalization and exchange rates of hundreds of crypto-currencies, including bitcoin.

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
A reference rate that can be used for institutional and contractual reference, provided as part of investment data feeds by the CME.

Chicago Mercantile Exchange Bitcoin Reference Rate:
一个参考汇率，可用于机构和合同参考，是CME作为投资数据的一部分提供的。

In addition to these various sites and applications, most bitcoin wallets will automatically convert amounts between bitcoin and other currencies. Joe will use his wallet to convert the price automatically before sending bitcoin to Alice.
除了这些网站和应用程序，大多数比特币钱包都能自动在比特币和其它货币之间实现转换。
在将比特币发送给Alice之前，Joe使用他的钱包来自动转换价格。

1.4.5发送和接收比特币

Alice has decided to exchange $10 US dollars for bitcoin, so as not to risk too much money on this new technology. She gives Joe $10 in cash, opens her Mycelium wallet application, and selects Receive. This displays a QR code with Alice's first bitcoin address.
Alice决定把10美元换成比特币，以免对这种新技术冒太多的风险。
她给了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，它有Alice的第一个比特币地址。

Joe then selects Send on his smartphone wallet and is presented with a screen containing two inputs:
- A destination bitcoin address
- The amount to send, in bitcoin (BTC) or his local currency (USD)

然后，Joe在他的手机钱包上选择Send，平布上会显示两个输入：
- 目的比特币地址
- 要发送的数额 （BTC或本地货币）

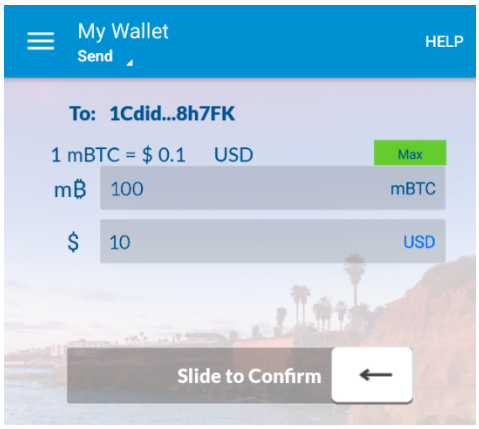

Figure 2. Airbitz mobile bitcoin wallet send screen
图1-2. Airbitz手机比特币钱包发送屏幕

In the input field for the bitcoin address, there is a small icon that looks like a QR code. This allows Joe to scan the barcode with his smartphone camera so that he doesn't have to type in Alice's bitcoin address, which is quite long and difficult to type. Joe taps the QR code icon and activates the smartphone camera, scanning the QR code displayed on Alice's smartphone.
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。
Joe可以用他的手机来扫描二维码，这样他就不必手工输入Alice的比特币地址，因为手工输入需要很长时间，而且容易出错。
Joe点击二维码图标并激活手机相机，扫描Alice手机上显示的二维码。

Joe now has Alice's bitcoin address set as the recipient. Joe enters the amount as $10 US dollars and his wallet converts it by accessing the most recent exchange rate from an online service. The exchange rate at the time is $100 US dollars per bitcoin, so $10 US dollars is worth 0.10 bitcoin (BTC), or 100 millibitcoin (mBTC) as shown in the screenshot from Joe's wallet (see Airbitz mobile bitcoin wallet send screen).
Joe现在已经将Alice的比特币地址设置为收款人。
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做转换。
当时的汇率是每个比特币$100美元，10美元值0.10 BTC，或100 mBTC。

Joe then carefully checks to make sure he has entered the correct amount, because he is about to transmit money and mistakes are irreversible. After double-checking the address and amount, he presses Send to transmit the transaction. Joe's mobile bitcoin wallet constructs a transaction that assigns 0.10 BTC to the address provided by Alice, sourcing

the funds from Joe's wallet and signing the transaction with Joe's private keys. This tells the bitcoin network that Joe has authorized a transfer of value to Alice's new address. As the transaction is transmitted via the peer-to-peer protocol, it quickly propagates across the bitcoin network. In less than a second, most of the well-connected nodes in the network receive the transaction and see Alice's address for the first time.
然后，Joe仔细做了检查，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。
仔细检查地址和金额后，他按Send来发送这个交易。
Joe的手机比特币钱包构建了一个交易：从Joe的钱包中将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的地址。
当交易通过P2P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收到交易，并且首次看到Alice的地址。

Meanwhile, Alice's wallet is constantly "listening" to published transactions on the bitcoin network, looking for any that match the addresses in her wallets. A few seconds after Joe's wallet transmits the transaction, Alice's wallet will indicate that it is receiving 0.10 BTC.
同时，Alice的钱包不断"监听"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的钱包将提示：它正在接收0.10 BTC。

Confirmations 确认

At first, Alice's address will show the transaction from Joe as "Unconfirmed." This means that the transaction has been propagated to the network but has not yet been recorded in the bitcoin transaction ledger, known as the blockchain. To be confirmed, a transaction must be included in a block and added to the blockchain, which happens every 10 minutes, on average. In traditional financial terms this is known as *clearing*. For more details on propagation, validation, and clearing (confirmation) of bitcoin transactions, see [mining].
最初，Alice的地址会把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目（区块链）中。
要确认交易，这个交易必须包含在一个区块中，并添加到区块链上，这种情况平均每10分钟发生一次。
在传统的财务术语中，这被称为"清算"。
有关下列的细节，请参考挖矿：比特币交易的传播、验证和清算（确认）。

Alice is now the proud owner of 0.10 BTC that she can spend. In the next chapter we will look at her first purchase with bitcoin, and examine the underlying transaction and propagation technologies in more detail.
Alice现在可以称自己是0.10 BTC的所有者，她能花费这些钱。
在下一章中，我们将看看她用比特币做了第一笔购买，更详细地研究底层交易和传播技术。