2比特币工作原理

How Bitcoin Works

2.1交易/区块/挖矿/区块链

The bitcoin system, unlike traditional banking and payment systems, is based on decentralized trust. Instead of a central trusted authority, in bitcoin, trust is achieved as an emergent property from the interactions of different participants in the bitcoin system.
“比特币系统”与传统的“银行业务”和“支付系统”不同，
它是基于“去中心化的信任”（分散的信任）。
在比特币中，信任不是一个中央可信机构，而是由比特币系统中不同参与者之间的互动而产生的一种自然出现的特性。

In this chapter, we will examine bitcoin from a high level by tracking a single transaction through the bitcoin system and watch as it becomes "trusted" and accepted by the bitcoin mechanism of distributed consensus and is finally recorded on the blockchain, the distributed ledger of all transactions. Subsequent chapters will delve into the technology behind transactions, the network, and mining.
在本章中，我们通过跟踪比特币系统中的一个交易，从一个高层次来考察比特币；
观察分布式共识的比特币机制如何信任和接受这个交易，并最终把它记录到区块链中，区块链是所有交易的分布式账本。
后面的章节将深入研究交易、网络和挖矿背后的技术。

2.1.1比特币概述

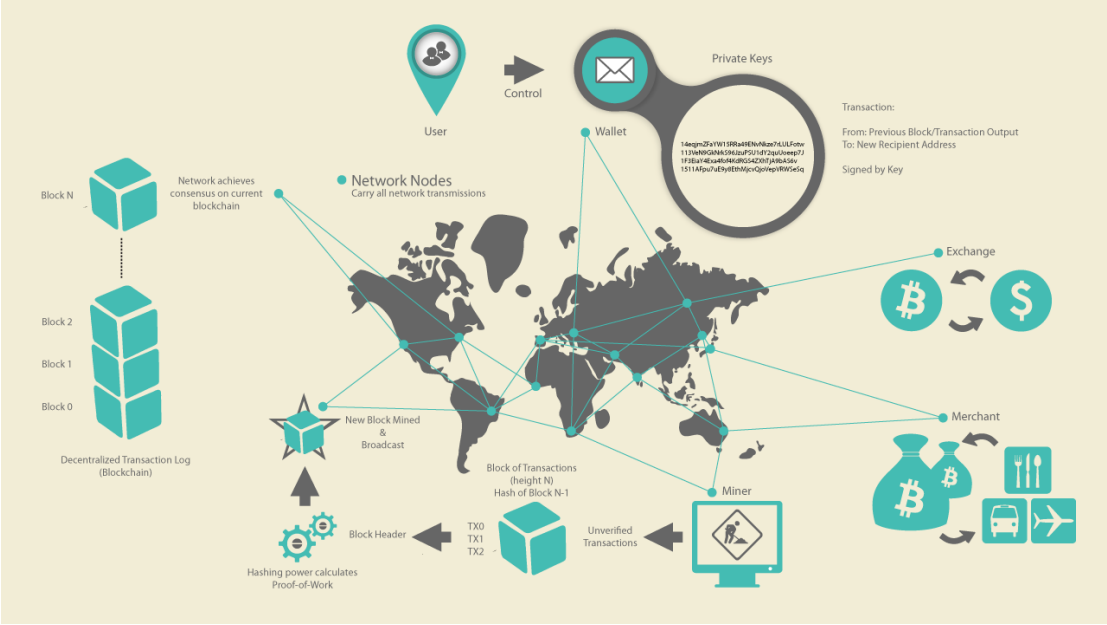

Figure 1. Bitcoin overview
图2-1比特币概览

In the overview diagram shown in Bitcoin Overview, we see that the bitcoin system consists of users with wallets containing keys, transactions that are propagated across the network, and miners who produce (through competitive computation) the consensus blockchain, which is the authoritative ledger of all transactions.
在图1所示的概览图中，“比特币系统”由下列组成：

- 用户：有包含密钥的钱包
- 交易：在网络上传播
- 矿工：通过竞争计算，生成共识区块链，这是所有交易的权威账目。

Each example in this chapter is based on an actual transaction made on the bitcoin network, simulating the interactions between the users (Joe, Alice, Bob, and Gopesh) by sending funds from one wallet to another. While tracking a transaction through the bitcoin network to the blockchain, we will use a *blockchain explorer* site to visualize each step. A blockchain explorer is a web application that operates as a bitcoin search engine, in that it allows you to search for addresses, transactions, and blocks and see the relationships and flows between them.
在本章中，每个例子都基于在比特币网络上进行的一个实际交易，
通过将资金从一个钱包发送到另一个钱包，来模拟用户（Joe、Alice、Bob和Gopesh）之间的交互。
在一个交易通过比特币网络到达区块链时，我们将使用一个区块链接浏览器网站，查看每个步骤。
一个区块链浏览器是一个web应用，它用作一个比特币搜索引擎，可用来搜索地址、交易和区块，查看它们之间的关系和流。

Popular blockchain explorers include:
常见的区块链浏览器有：

- BlockCypher Explorer https://live.blockcypher.com/
- blockchain.info https://blockchain.info/
- BitPay Insight https://insight.bitpay.com/

Each of these has a search function that can take a bitcoin address, transaction hash, block number, or block hash and retrieve corresponding information from the bitcoin network. With each transaction or block example, we will provide a URL so you can look it up yourself and study it in detail.
每个区块链浏览器都有一个搜索功能，能够用一个比特币地址、交易哈希、区块号或区块哈希，从比特币网络获得对应的信息。
对于每个交易或区块例子，我们会提供一个URL，这样你可以查看和研究细节。

2.1.2买一杯咖啡

Alice, introduced in the previous chapter, is a new user who has just acquired her first bitcoin. In [getting_first_bitcoin], Alice met with her friend Joe to exchange some cash for bitcoin. The transaction created by Joe funded Alice’s wallet with 0.10 BTC. Now Alice will make her first retail transaction, buying a cup of coffee at Bob’s coffee shop in Palo Alto, California.
Alice是一个新用户，刚获得了第一个比特币。
Alice和Joe见面时，用现金换取了比特币。由Joe创建的这个交易向Alice的钱包转了0.10 BTC。
现在，Alice将第一次使用比特币在Bob的咖啡店买一杯咖啡。

Bob’s Cafe recently started accepting bitcoin payments by adding a bitcoin option to its point-of-sale system. The prices at Bob’s Cafe are listed in the local currency (US dollars), but at the register, customers have the option of paying in either dollars or bitcoin. Alice places her order for a cup of coffee and Bob enters it into the register, as he does for all transactions. The point-of-sale system automatically converts the total price from US dollars to bitcoin at the prevailing market rate and displays the price in both currencies:
Bob的咖啡店最近开始接受比特币支付，他在销售点系统中增加了一个比特币选项。
咖啡店中价格是用美元标示的，但在收银机上，顾客可以选择用美元或比特币支付。
Alice点了一杯咖啡，Bob将交易输入收银机，就像做其它交易一样。

之后，销售点系统自动按照当前市场汇率把美元转换成比特币，并显示两种货币的价格：

```
Total:
$1.50 USD
0.015 BTC
```

Bob says, "That's one-dollar-fifty, or fifteen millibits."
Bob说：总共1.50美元，或0.015比特币。

Bob's point-of-sale system will also automatically create a special QR code containing a *payment request* (see Payment request QR code).
Bob的销售点系统还将自动创建一个二维码，它包含一个付款请求。

Unlike a QR code that simply contains a destination bitcoin address, a payment request is a QR-encoded URL that contains a destination address, a payment amount, and a generic description such as "Bob's Cafe." This allows a bitcoin wallet application to prefill the information used to send the payment while showing a human-readable description to the user. You can scan the QR code with a bitcoin wallet application to see what Alice would see.
这个支付请求二维码并不是只包含一个目的比特币地址，它是一个二维编码的URL，包含有一个目的地址、一个支付金额、和一个描述（例如"Bob的咖啡店"）。
这样，比特币钱包应用程序在给用户显示可读描述时，可以预先填写信息，这些信息用于发送这个支付。
你可以用比特币钱包应用程序扫描这个二维码，看看Alice看到的信息。

Figure 2. Payment request QR code
图2-2支付请求二维码

```
Tip: Try to scan this with your wallet to see the address and amount but DO
NOT SEND MONEY.
```
提示：尝试用你的钱包扫描这个二维码，看看它的地址和金额，但不要支付。

The payment request QR code encodes the following URL, defined in BIP-21:
根据BIP-21的定义，这个支付请求二维码编码了下面的URL：
ddk问题：URL是什么?

```
bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA?
amount=0.015&
label=Bob%27s%20Cafe&
message=Purchase%20at%20Bob%27s%20Cafe

Components of the URL

A bitcoin address: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA"
The payment amount: "0.015"
A label for the recipient address: "Bob's Cafe"
A description for the payment: "Purchase at Bob's Cafe"
```

Alice uses her smartphone to scan the barcode on display. Her smartphone shows a payment of 0.0150 BTC to Bob's Cafe and she selects Send to authorize the payment. Within a few seconds (about the same amount of time as a credit card authorization), Bob sees the transaction on the register, completing the transaction.
Alice用手机扫描了这个二维码。
手机显示一个给Bob咖啡店的0.0150比特币的支付，然后她按下Send以授权支付。
在几秒内（与信用卡授权所需时间基本相同），Bob会在收银机看到这笔交易，交易完成。

In the following sections, we will examine this transaction in more detail. We'll see how Alice's wallet constructed it, how it was propagated across the network, how it was verified, and finally, how Bob can spend that amount in subsequent transactions.
在后面的小节中，我们将更详细地研究这个交易。
我们要看看，Alice的钱包如何构建这个交易，如何在网络上传播这个交易，这个交易如何被验证，Bob如何能在以后的交易中花费这笔钱。

Note: The bitcoin network can transact in fractional values, e.g., from millibitcoin (1/1000th of a bitcoin) down to 1/100,000,000th of a bitcoin, which is known as a satoshi. Throughout this book, we'll use the term "bitcoin" to refer to any quantity of bitcoin currency, from the smallest unit (1 satoshi) to the total number (21,000,000) of all bitcoin that will ever be mined.
注意：比特币网络可以交易很小的金额，例如从1/1000比特币(1毫）到一亿分之一比特币（1聪）。在本书中，我们将用"比特币"表示任意数量的比特币货币，从最小单位（1聪）到比特币总量（2100,0000）。

You can examine Alice's transaction to Bob's Cafe on the blockchain using a block explorer site (View Alice's transaction on blockchain.info):
你可以使用区块浏览器查看Alice的这个交易。

Example 1. View Alice's transaction on blockchain.info
例1. 查看Alice的交易

```
https://blockchain.info/tx/
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
```

2.2 比特币交易

In simple terms, a transaction tells the network that the owner of some bitcoin value has authorized the transfer of that value to another owner. The new owner can now spend the bitcoin by creating another transaction that authorizes the transfer to another owner, and so on, in a chain of ownership.
简单来说，一个交易告知网络：比特币的持有者已授权把比特币转帐给其他人。
新持有者可以通过创建另一个交易把来花费比特币，将其转移给另一个人，这样就形成了一个所有权链。

2.2.1交易输入和输出

Transactions are like lines in a double-entry bookkeeping ledger. Each transaction contains one or more "inputs," which are like debits against a bitcoin account. On the other side of the transaction, there are one or more "outputs," which are like credits added to a bitcoin account. The inputs and outputs (debits and credits) do not necessarily add up to the same amount. Instead, outputs add up to slightly less than inputs and the difference represents an implied *transaction fee*, which is a small payment collected by the miner who includes the transaction in the ledger.
交易就像复式记账法中的行。
每个交易包含一个或多个“输入”，输入就像一个比特币账户的收入（debit）。
这个交易还有一个或多个“输出”，输出就像是一个比特币账户的支出（credit）。
输入总额和输出总额不必相等。当输出少于输入时，差额就是“矿工费”，矿工在将交易放入账本时可以获得这笔费用。

A bitcoin transaction is shown as a bookkeeping ledger entry in Transaction as double-entry bookkeeping.
如图2-3显示的是一个比特币交易的复式账目。

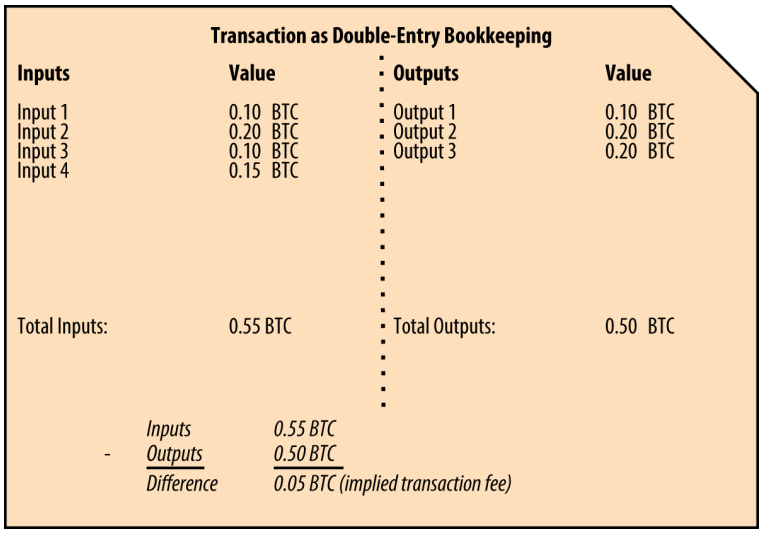

Figure 3. Transaction as double-entry bookkeeping
图2-3交易就像复式记账

The transaction also contains proof of ownership for each amount of bitcoin (inputs) whose value is being spent, in the form of a digital signature from the owner, which can be independently validated by anyone. In bitcoin terms, "spending" is signing a transaction that transfers value from a previous transaction over to a new owner identified by a bitcoin address.
这个交易还包含了每个输入的所有权证明，用的是所有者的数字签名，可以被任何人独立验证。

在比特币术语中，“消费”是签署一个交易，它将来自前一个交易的钱转给一个新的所有者（用比特币地址标识）。

2.2.2交易链

Alice’s payment to Bob’s Cafe uses a previous transaction’s output as its input. In the previous chapter, Alice received bitcoin from her friend Joe in return for cash. That transaction created a bitcoin value locked by Alice’s key. Her new transaction to Bob’s Cafe references the previous transaction as an input and creates new outputs to pay for the cup of coffee and receive change.
Alice向Bob支付时，使用之前交易的一个输出作为本次交易的输入。
在前一章中，Alice从Joe那里用现金换了一些比特币。
那个交易创建了一些被Alice的密钥锁定的比特币。
Alice用之前的这个交易作为本次交易的输入，并创建新的输出来向Bob支付和获得找零。

The transactions form a chain, where the inputs from the latest transaction correspond to outputs from previous transactions. Alice’s key provides the signature that unlocks those previous transaction outputs, thereby proving to the bitcoin network that she owns the funds. She attaches the payment for coffee to Bob’s address, thereby "encumbering" that output with the requirement that Bob produces a signature in order to spend that amount. This represents a transfer of value between Alice and Bob. This chain of transactions, from Joe to Alice to Bob, is illustrated in A chain of transactions, where the output of one transaction is the input of the next transaction.
这些交易形成了一条链，最近交易的输入对应以前交易的输出。
Alice的密钥提供了签名，签名解锁之前交易的输出，这就向比特币网络证明了她拥有这笔钱。
Alice将这笔钱支付给Bob的地址，从而保护了这个输出，必须有Bob的签名才能消费这笔钱。
这就是Alice和Bob之间钱的转移。下图显示了从Joe到Alice再到Bob的交易链。

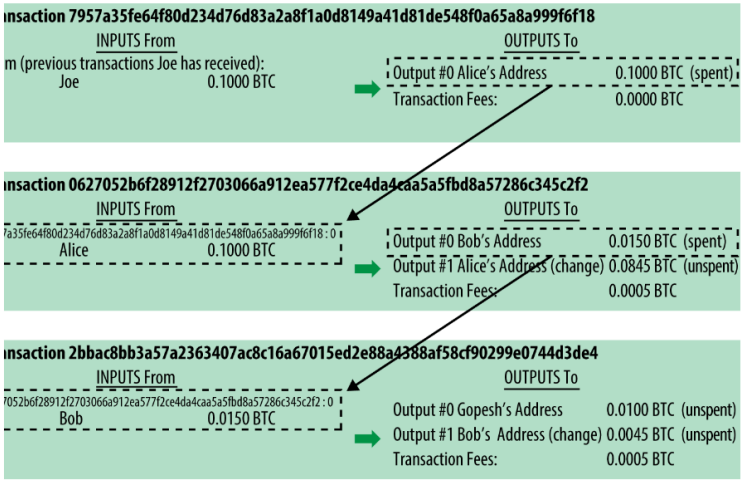

Figure 4. A chain of transactions, where the output of one transaction is the input of the next transaction
图4.一个交易链，一个交易的输出是下一个交易的输入

2.2.3找零

Many bitcoin transactions will include outputs that reference both an address of the new owner and an address of the current owner, called the *change* address. This is because transaction inputs, like currency notes, cannot be divided. If you purchase a $5 US dollar item in a store but use a $20 US dollar bill to pay for the item, you expect to receive $15

US dollars in change. The same concept applies to bitcoin transaction inputs. If you purchased an item that costs 5 bitcoin but only had a 20 bitcoin input to use, you would send one output of 5 bitcoin to the store owner and one output of 15 bitcoin back to yourself as change (less any applicable transaction fee). Importantly, the change address does not have to be the same address as that of the input and for privacy reasons is often a new address from the owner's wallet.
许多比特币交易都会包含新所有者的地址（卖方地址）和当前所有者的地址（找零地址）的输出。
这是因为，交易的输入就像纸币一样，不能被分割。
如果你到商店买5美元的东西，给了商家20美元，商家会找你15美元。
这种概念也适用于比特币交易的输入。如果你要支付5比特币，但你只能使用20比特币的输入，那么，一个输出是给商家的5比特币，另一个输出是给自己的15比特币（减去交易费）。
重要的是，找零地址不必与输入地址相同，为了保护隐私，通常是所有者钱包中的一个新地址。

Different wallets may use different strategies when aggregating inputs to make a payment requested by the user. They might aggregate many small inputs, or use one that is equal to or larger than the desired payment. Unless the wallet can aggregate inputs in such a way to exactly match the desired payment plus transaction fees, the wallet will need to generate some change. This is very similar to how people handle cash. If you always use the largest bill in your pocket, you will end up with a pocket full of loose change. If you only use the loose change, you'll always have only big bills. People subconsciously find a balance between these two extremes, and bitcoin wallet developers strive to program this balance.
为了支付而汇总输入时，不同的钱包可以使用不同的策略。
它可能会聚合许多小输入，或者使用一个输入（大于等于所需付款）。
除非钱包能使输入等于输出加交易费，否则钱包需要产生一些找零。
这与人们处理现金非常相似。如果你总是用最大面额支付，你的钱包会有很多零钱。
如果你只使用零钱，你就总是只有大钞。
人们在潜意识中总是在这两个极端之间找到平衡，而比特币钱包开发者也力图实现这种平衡。

In summary, *transactions* move value from *transaction inputs* to *transaction outputs*. An input is a reference to a previous transaction's output, showing where the value is coming from. A transaction output directs a specific value to a new owner's bitcoin address and can include a change output back to the original owner. Outputs from one transaction can be used as inputs in a new transaction, thus creating a chain of ownership as the value is moved from owner to owner (see A chain of transactions, where the output of one transaction is the input of the next transaction).
总之，交易是将钱从交易输入移至交易输出。
一个输入指向一个之前交易的输出，说明这个钱来自哪儿。
交易输出将指定金额发送给新所有者的比特币地址，还可以有一个找零输出。
一笔交易的输出可以被用作另一笔交易的输入，这样，随着钱从一个地址移动到另一个地址，就形成了一条所有权链。

2.2.4 常见的交易形式

The most common form of transaction is a simple payment from one address to another, which often includes some "change" returned to the original owner. This type of transaction has one input and two outputs and is shown in Most common transaction.
最常见的交易形式是从一个地址到另一个地址的简单支付，这种交易也常常包含“找零”。
这种交易有一个输入和两个输出，如图2-5所示。

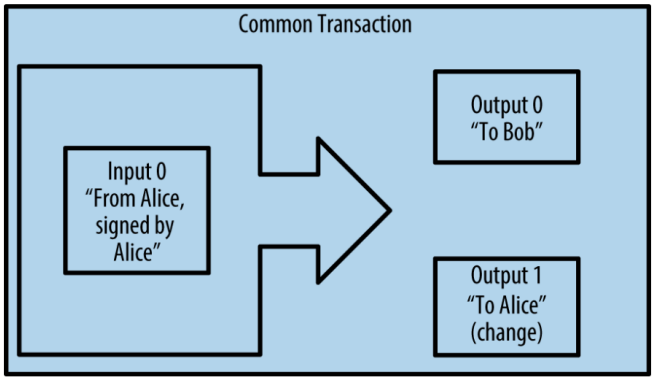

Figure 5. Most common transaction

Another common form of transaction is one that aggregates several inputs into a single output (see Transaction aggregating funds). This represents the real-world equivalent of exchanging a pile of coins and currency notes for a single larger note. Transactions like these are sometimes generated by wallet applications to clean up lots of smaller amounts that were received as change for payments.
另一种常见的交易形式是，汇集多个输入到一个输出（图2-6）。
这相当于把很多零钱兑换为一张大额钞票。
像这样的交易有时是由钱包应用程序产生，用来清理大量小额，他们是作为支付找零收取的。

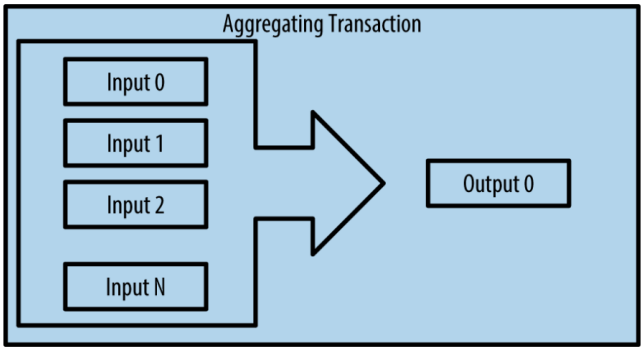

Figure 6. Transaction aggregating funds

Finally, another transaction form that is seen often on the bitcoin ledger is a transaction that distributes one input to multiple outputs representing multiple recipients (see Transaction distributing funds). This type of transaction is sometimes used by commercial entities to distribute funds, such as when processing payroll payments to multiple employees.
最后，另一种在比特币账目中常见的交易形式是，将一个输入分配给多个输出（图2-7）。
这类交易有时被商业实体用于分配资金，例如给员工发工资。

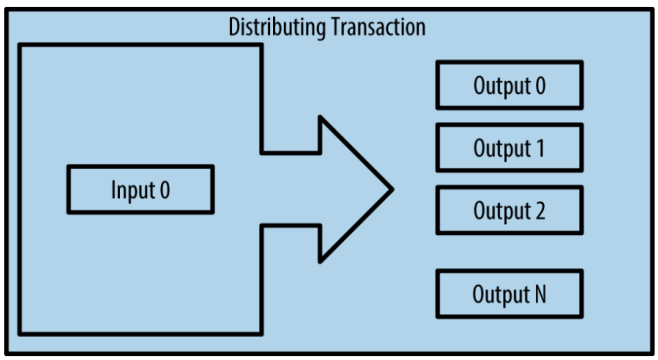

Figure 7. Transaction distributing funds

2.3 构建一个交易

Alice's wallet application contains all the logic for selecting appropriate inputs and outputs to build a transaction to Alice's specification. Alice only needs to specify a destination and an amount, and the rest happens in the wallet application without her seeing the details. Importantly, a wallet application can construct transactions even if it is completely offline. Like writing a check at home and later sending it to the bank in an envelope, the transaction does not need to be constructed and signed while connected to the bitcoin network.
Alice的钱包应用程序包含所有的逻辑：按照Alice的要求，选择合适的输入和输出，来构建一个交易。
Alice只需要指定一个目标地址和一个金额，其余的事情由钱包应用程序完成，不需要她关心细节。
重要的是，即使钱包应用程序不在线，它也能构建交易。
就像在家写了一张支票，然后放到信封里发给银行一样，不用连接到比特币网络，也能构建和签名交易。

2.3.1 获取正确的输入

Alice's wallet application will first have to find inputs that can pay the amount she wants to send to Bob. Most wallets keep track of all the available outputs belonging to addresses in the wallet. Therefore, Alice's wallet would contain a copy of the transaction output from Joe's transaction, which was created in exchange for cash (see [getting_first_bitcoin]).
Alice的钱包应用程序首先要找到能够支付的输入。
大多数钱包应用程序跟踪着钱包中这些地址的所有可用输出。
因此，Alice的钱包包含她购买比特币交易的交易输出。

A bitcoin wallet application that runs as a full-node client actually contains a copy of every unspent output from every transaction in the blockchain. This allows a wallet to construct transaction inputs as well as quickly verify incoming transactions as having correct inputs. However, because a full-node client takes up a lot of disk space, most user wallets run "lightweight" clients that track only the user's own unspent outputs.
当比特币钱包应用程序作为一个全节点客户端运行时，它实际包含了区块链中每个交易的未花费输出。
这使得钱包能够构建交易输入，又能快速验证收到的交易有争取的输入。
但是，全节点客户端占用硬盘空间太大，所以，多数用户钱包运行轻量级客户端，它只跟踪用户自己的未花费输出。

If the wallet application does not maintain a copy of unspent transaction outputs, it can query the bitcoin network to retrieve this information using a variety of APIs available by different providers or by asking a full-node using an application programming interface (API) call. Look up all the unspent outputs for Alice's bitcoin address shows an API request, constructed as an HTTP GET command to a specific URL. This URL will return all the unspent transaction outputs for an address, giving any application the information it needs to construct transaction inputs for spending. We use the simple command-line HTTP client *cURL* to retrieve the response.
如果钱包应用程序没有未花费交易输出，它可以通过查询比特币网络来获得这个信息，方法是使用不同提供商的各种API，或者使用API向全节点询问。
例2-1显示了一个API请求，它被构造为到一个特定URL的一个HTTP GET命令。
这个URL会返回某个地址的所有未花费交易输出，为应用程序提供构造交易输入所需的信息。
我们使用一个简单的命令行HTTP客户端 cURL来获得这个响应。

Example 2. Look up all the unspent outputs for Alice's bitcoin address
例2-1 查找Alice的比特币地址所有的未花费输出

```
$ curl https://blockchain.info/unspent?
active=1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
{
```

```
   "unspent_outputs":[
   {
        "tx_hash"         : "186f9f998a5...2836dd734d2804fe65fa35779",
        "tx_index"        : 104810202,
        "tx_output_n"     : 0,
        "script"          :
"76a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac",
        "value"           : 10000000,
        "value_hex"       : "00989680",
        "confirmations"   : 0
   }
   ]
}
```

The response in Look up all the unspent outputs for Alice's bitcoin address shows one unspent output (one that has not been redeemed yet) under the ownership of Alice's address 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK. The response includes the reference to the transaction in which this unspent output is contained (the payment from Joe) and its value in satoshis, at 10 million, equivalent to 0.10 bitcoin. With this information, Alice's wallet application can construct a transaction to transfer that value to new owner addresses.
例2-1的响应数据显示了在Alice的地址 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK 上有一个未花费输出。
这个响应包含对一个交易的引用，这个交易包含未花费输出（Joe的支付）和它的价值（0.10比特币）
通过这个信息，Alice的钱包应用程序就可以创建新的交易，将钱转到新地址。

Tip: View the transaction from Joe to Alice.
提示：查看从Joe到Alice的交易。

As you can see, Alice's wallet contains enough bitcoin in a single unspent output to pay for the cup of coffee. Had this not been the case, Alice's wallet application might have to "rummage" through a pile of smaller unspent outputs, like picking coins from a purse until it could find enough to pay for the coffee. In both cases, there might be a need to get some change back, which we will see in the next section, as the wallet application creates the transaction outputs (payments).
如你所见，Alice的钱包在一个未花费输出中有足够的比特币来支付一杯咖啡。
如果不够，钱包就得搜寻一些小的未花费输出，就像从存钱罐里找硬币一样，找到足够支付咖啡的钱。
两种情况可能都需要找回零钱，而这些找零也是钱包所创建的交易的输出的组成部分。下一节会有所描述。

2.3.2 创建输出

A transaction output is created in the form of a script that creates an encumbrance on the value and can only be redeemed by the introduction of a solution to the script. In simpler terms, Alice's transaction output will contain a script that says something like, "This output is payable to whoever can present a signature from the key corresponding to Bob's public address." Because only Bob has the wallet with the keys corresponding to that address, only Bob's wallet can present such a signature to redeem this output. Alice will therefore "encumber" the output value with a demand for a signature from Bob.
交易输出被创建成为脚本形式，使得输出的钱只能通过这个脚本的一个解才能被花费。
简单地说，Alice的交易输出包含一个脚本，这个脚本说：谁能拿出一个与Bob的公开地址相匹配的签名，能花费这个输出的钱。
因为只有Bob钱包中的私钥可以匹配这个地址，所以只有Bob的钱包可以提供这个签名以花费这笔钱。
因此，Alice通过要求Bob的签名来保护这个输入中的钱。

This transaction will also include a second output, because Alice's funds are in the form of a 0.10 BTC output, too much money for the 0.015 BTC cup of coffee. Alice will need 0.085 BTC in change. Alice's change payment is created by Alice's wallet as an output in the very

same transaction as the payment to Bob. Essentially, Alice's wallet breaks her funds into two payments: one to Bob and one back to herself. She can then use (spend) the change output in a subsequent transaction.
这个交易还包含另一个输出。
因为Alice有0.10比特币，而咖啡只需0.015 比特币，需要找给Alice 0.085比特币。
Alice钱包在这个交易中创建一个找零支付。
可以说，Alice的钱包将她的钱分成了两个支付：一个给Bob，一个给自己。
她可以在以后的交易中消费这笔零钱输出。

Finally, for the transaction to be processed by the network in a timely fashion, Alice's wallet application will add a small fee. This is not explicit in the transaction; it is implied by the difference between inputs and outputs. If instead of taking 0.085 in change, Alice creates only 0.0845 as the second output, there will be 0.0005 BTC (half a millibitcoin) left over. The input's 0.10 BTC is not fully spent with the two outputs, because they will add up to less than 0.10. The resulting difference is the *transaction fee* that is collected by the miner as a fee for validating and including the transaction in a block to be recorded on the blockchain.
最后，为了让这笔交易及时被网络处理，Alice的钱包会多付一小笔费用。
这笔费用没有明显地包含在交易中的，而是隐含在输入和输出的差额中。
如果Alice创建找零时只找 0.0845比特币，而不是 0.085比特币，就剩下 0.0005比特币。
因为输出加起来小于 0.10比特币，所以输入没有被完全消费。
这个差值会就被矿工当作交易费放到区块的交易里，最终放进区块链账目中。

The resulting transaction can be seen using a blockchain explorer web application, as shown in [Alice's transaction to Bob's Cafe](#).
可以使用区块链浏览器web应用程序查看这个交易。

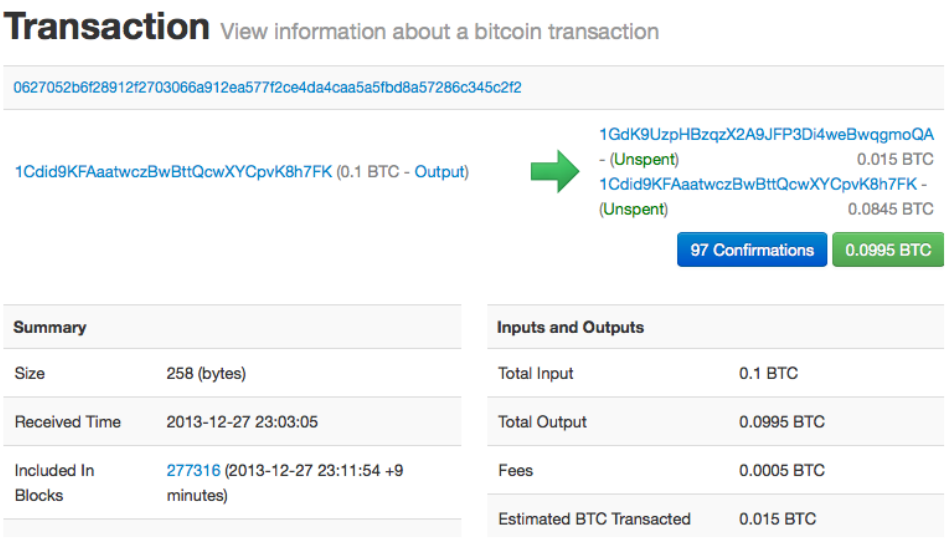

Figure 8. Alice's transaction to Bob's Café

Tip: View the transaction from Alice to Bob's Cafe.
提示：查看从Alice到Bob的交易。

2.3.3 把交易加入账目

The transaction created by Alice's wallet application is 258 bytes long and contains everything necessary to confirm ownership of the funds and assign new owners. Now, the transaction must be transmitted to the bitcoin network where it will become part of the blockchain.

这个被Alice钱包应用程序创建的交易有258字节，包含了确认资金所有权和分配给新所有者所需要的全部信息。
现在，这个交易必须要被传送到比特币网络，它将成为区块链的一部分。

In the next section we will see how a transaction becomes part of a new block and how the block is "mined." Finally, we will see how the new block, once added to the blockchain, is increasingly trusted by the network as more blocks are added.
在下一节，我们将看到，一个交易如何成为新区块的一部分，以及区块如何被挖矿。
最后，我们会看看，新区块（一旦被加入区块链后）是如何随着更多区块被加入而增加可信度的。

2.3.3.1 发送交易

Because the transaction contains all the information necessary to process, it does not matter how or where it is transmitted to the bitcoin network. The bitcoin network is a peer-to-peer network, with each bitcoin client participating by connecting to several other bitcoin clients. The purpose of the bitcoin network is to propagate transactions and blocks to all participants.
因为这个交易包含处理所需的所有信息，所以它是被如何或从哪里传送到比特币网络就无所谓了。
比特币网络是一个P2P网络，每个比特币客户端通过与其它几个比特币客户端连接来加入。
比特币网络的目的是向所有参与者传播交易和区块。

2.3.3.2 如何传播

Any system, such as a server, desktop application, or wallet, that participates in the bitcoin network by "speaking" the bitcoin protocol is called a *bitcoin node*. Alice's wallet application can send the new transaction to any bitcoin node it is connected to over any type of connection: wired, WiFi, mobile, etc. Her bitcoin wallet does not have to be connected to Bob's bitcoin wallet directly and she does not have to use the internet connection offered by the cafe, though both those options are possible, too. Any bitcoin node that receives a valid transaction it has not seen before will immediately forward it to all other nodes to which it is connected, a propagation technique known as *flooding*. Thus, the transaction rapidly propagates out across the peer-to-peer network, reaching a large percentage of the nodes within a few seconds.
通过说比特币协议来参与比特币网络的任何系统（例如服务器、桌面应用程序、钱包），都被称为比特币节点。
Alice的钱包应用程序可以通过任何类型的连接（有线、WiFi、移动等）向它连接的比特币节点发送这个新交易。
她的钱包不必与Bob的钱包直接连接，也不必使用咖啡店提供的互联网连接，虽然这两者都是可能的。
任何比特币网络节点收到一个之前没见过的有效交易时，会立刻将它转发给连接的其它节点。
因此，这个交易迅速地在P2P网络中传播，几秒内就能到达大多数节点。

2.3.3.3 Bob的视角

If Bob's bitcoin wallet application is directly connected to Alice's wallet application, Bob's wallet application might be the first node to receive the transaction. However, even if Alice's wallet sends the transaction through other nodes, it will reach Bob's wallet within a few seconds. Bob's wallet will immediately identify Alice's transaction as an incoming payment because it contains outputs redeemable by Bob's keys. Bob's wallet application can also independently verify that the transaction is well formed, uses previously unspent inputs, and contains sufficient transaction fees to be included in the next block. At this point Bob can assume, with little risk, that the transaction will shortly be included in a block and confirmed.
如果Bob的钱包是直接连接Alice的钱包，Bob的钱包也许就是第一个收到这个交易的节点。
但是，即使Alice的交易是从通过其它节点转发过来的，也可以在几秒钟内到达Bob的钱包。
Bob的钱包会立即认出 Alice的交易是一个收入支付，因为它包含能用Bob的私钥花费的输出。
Bob的钱包也能独立地用之前未消费输出来确认这个交易是正确构建的，并且包含足够交易费，能使它被下一个区块包含进去。

这时，Bob可以认为（风险很小）这个交易会很快被加到一个区块中，并被确认。

ddk问题：uses previously unspent inputs是否应该是output?

Tip：A common misconception about bitcoin transactions is that they must be "confirmed" by waiting 10 minutes for a new block, or up to 60 minutes for a full six confirmations. Although confirmations ensure the transaction has been accepted by the whole network, such a delay is unnecessary for small-value items such as a cup of coffee. A merchant may accept a valid small-value transaction with no confirmations, with no more risk than a credit card payment made without an ID or a signature, as merchants routinely accept today.

提示：对比特币交易的一个常见误解是，必须要等10分钟后被确认加进一个新区块，或等60分钟以得到六次确认后才是有效的。

虽然这些确认可以确保交易已被整个网络接受，但对于像一杯咖啡这样的小额商品来说，就没有必要等待那么长时间了。商家可以免确认来接受比特币小额支付。这样做并不比接受一个没有签名的信用卡的风险更大，而后者是现在商家常做的事情。

2.4 比特币挖矿

Alice's transaction is now propagated on the bitcoin network. It does not become part of the *blockchain* until it is verified and included in a block by a process called *mining*. See [mining] for a detailed explanation.
Alice的交易现在被传播到比特币网络上了。
但只有被证实，并且被挖矿过程包含在一个区块中后，这个交易才会成为区块链的一部分。
关于挖矿的详细描述见第10章。

The bitcoin system of trust is based on computation. Transactions are bundled into *blocks*, which require an enormous amount of computation to prove, but only a small amount of computation to verify as proven. The mining process serves two purposes in bitcoin:
可信的比特币系统是建立在计算的基础上。
交易被打包到区块中，这需要大量的计算来证明，但只需少量计算就能验证它们已被证明。
挖矿在比特币中有两个目的：

- Mining nodes validate all transactions by reference to bitcoin's *consensus rules*. Therefore, mining provides security for bitcoin transactions by rejecting invalid or malformed transactions.

  挖矿节点通过比特币的共识规则验证所有交易。
  因此，通过通过拒绝无效或畸形交易，挖矿为比特币交易提供了安全性。

- Mining creates new bitcoin in each block, almost like a central bank printing new money. The amount of bitcoin created per block is limited and diminishes with time, following a fixed issuance schedule.

  挖矿在每个区块中创造新的比特币，就像中央银行印发新钱一样。
  每个区块创造的比特币数量是有限的，按照固定的发行计划，随时间会渐渐减少。

Mining achieves a fine balance between cost and reward. Mining uses electricity to solve a mathematical problem. A successful miner will collect a *reward* in the form of new bitcoin and transaction fees. However, the reward will only be collected if the miner has correctly validated all the transactions, to the satisfaction of the rules of *consensus*. This delicate balance provides security for bitcoin without a central authority.
挖矿在成本和报酬之间实现了一个良好的平衡。
挖矿使用电力来解决一个数学问题。一个成功的矿工获得奖励的方式是：新的比特币和交易费。
但是，只有矿工正确验证了所有的交易，满足共识规则，才能获得奖励。
这种微妙的平衡为没有中央机构的比特币提供了安全性。

A good way to describe mining is like a giant competitive game of sudoku that resets every time someone finds a solution and whose difficulty automatically adjusts so that it takes approximately 10 minutes to find a solution. Imagine a giant sudoku puzzle, several thousand rows and columns in size. If I show you a completed puzzle you can verify it quite quickly. However, if the puzzle has a few squares filled and the rest are empty, it takes a lot of work to solve! The difficulty of the sudoku can be adjusted by changing its size (more or fewer rows and columns), but it can still be verified quite easily even if it is very large. The "puzzle" used in bitcoin is based on a cryptographic hash and exhibits similar characteristics: it is asymmetrically hard to solve but easy to verify, and its difficulty can be adjusted.
描述挖矿的一个方法是，将它看做为多人参与的一个巨大的数独游戏。
一旦有人发现了正确的解之后，数独游戏会自动调整难度，以使游戏每次需要大约10分钟才能解决。
想象一个有几千行几千列的巨大数独游戏。
如果给你一个已经完成的数独，你可以很快地验证它。
然而，如果这个数独只有几个方格里有数字，其余方格都为空的话，就要花费很长的时间来解决。
这个数独游戏的困难度可以通过改变其大小（m行*n列）来调整，但即使非常大，验证它也是相当容易。

比特币中的 "谜题" 是基于哈希加密算法，它展现了相似的特性：解起来困难，但验证很容易，并且其困难度可以调整。

In [user-stories], we introduced Jing, an entrepreneur in Shanghai. Jing runs a *mining farm*, which is a business that runs thousands of specialized mining computers, competing for the reward. Every 10 minutes or so, Jing's mining computers compete against thousands of similar systems in a global race to find a solution to a block of transactions. Finding such a solution, the so-called *Proof-of-Work* (PoW), requires quadrillions of hashing operations per second across the entire bitcoin network. The algorithm for Proof-of-Work involves repeatedly hashing the header of the block and a random number with the SHA256 cryptographic algorithm until a solution matching a predetermined pattern emerges. The first miner to find such a solution wins the round of competition and publishes that block into the blockchain.
前面场景中我们提到了Jing，他在比特币网络中扮演了一个矿工的角色。
大概每10分钟，Jing和其他上千个矿工一起展开一场对一个区块寻找正解的全球竞赛。
为寻找这个解（也称工作量证明），整个网络需要每秒亿万次哈希计算的能力。
这个工作量证明算法是用SHA256加密算法不断地对“区块头和一个随机数”进行哈希计算，直到找到一个和预设值相匹配的解。
第一个找到这个解的矿工会赢得这局竞赛，并将它的区块发布到区块链中。

Jing started mining in 2010 using a very fast desktop computer to find a suitable Proof-of-Work for new blocks. As more miners started joining the bitcoin network, the difficulty of the problem increased rapidly. Soon, Jing and other miners upgraded to more specialized hardware, such as high-end dedicated graphical processing units (GPUs) cards such as those used in gaming desktops or consoles. At the time of this writing, the difficulty is so high that it is profitable only to mine with application-specific integrated circuits (ASIC), essentially hundreds of mining algorithms printed in hardware, running in parallel on a single silicon chip. Jing's company also participates in a *mining pool*, which much like a lottery pool allows several participants to share their efforts and rewards. Jing's company now runs a warehouse containing thousands of ASIC miners to mine for bitcoin 24 hours a day. The company pays its electricity costs by selling the bitcoin it is able to generate from mining, creating some income from the profits.
Jing从2010年开始挖矿，当时他使用一个非常快的桌面计算机来为新区块寻找正解。
随着越来越多的矿工加入比特币网络，寻找谜题正解的困难度迅速增大。
不久，Jing和其他矿工升级成更专业的硬件，比如游戏桌面电脑或控制台专用的高端独享GPU芯片。
在写本书时，解题已经变得极其困难，只有使用集成了几百个挖矿专用算法硬件，并能同时在一个单独芯片上并行工作的专用集成电路（ASIC），挖矿才会营利。
Jing同时加入了一个能够让多个矿工共享计算力和报酬的矿池。
Jing现在运行两个通过USB联接的ASIC机器，每天24小时不间断地挖矿。
他卖掉一些挖矿所得到的比特币来支付电费，并获得一些收入。

2.5 Mining Transactions in Blocks

New transactions are constantly flowing into the network from user wallets and other applications. As these are seen by the bitcoin network nodes, they get added to a temporary pool of unverified transactions maintained by each node. As miners construct a new block, they add unverified transactions from this pool to the new block and then attempt to prove the validity of that new block, with the mining algorithm (Proof-of-Work). The process of mining is explained in detail in [mining].
新交易不断地从用户钱包和其它应用程序流入比特币网络。
当比特币网络上的节点看到这些交易时，会先将它们放到自己维护的一个临时的未经验证的交易池中。
当矿工构建一个新区块时，会从这个交易池中拿出一些交易放到新区块中，然后通过尝试解决一个非常困难的问题（工作量证明），以证明这个新区块的合法性。

Transactions are added to the new block, prioritized by the highest-fee transactions first and a few other criteria. Each miner starts the process of mining a new block of transactions as soon as he receives the previous block from the network, knowing he has

lost that previous round of competition. He immediately creates a new block, fills it with transactions and the fingerprint of the previous block, and starts calculating the Proof-of-Work for the new block.
这些交易被加进新区块时，以交易费和其它的一些规则进行排序。
矿工一旦从网络上收到一个新区块时，会意识到：在这个区块上的解题竞赛已经输掉了，要马上开始下一个新区块的挖矿工作。
它会立刻将一些交易和这个新区块的数字指纹放在一起开始构建下一个新区块，并开始为它计算工作量证明。

Each miner includes a special transaction in his block, one that pays his own bitcoin address the block reward (currently 12.5 newly created bitcoin) plus the sum of transaction fees from all the transactions included in the block. If he finds a solution that makes that block valid, he "wins" this reward because his successful block is added to the global blockchain and the reward transaction he included becomes spendable.
每个矿工会在他的区块中包含一个特殊的交易，将新生成的比特币（当前每个区块为12.5比特币）作为奖励支付到他自己的比特币地址，再加上区块中所有交易的交易费的总和作为自己的奖励。
如果他找到了使新区块有效的解法，他就会得到这些奖励，因为这个新区块被加入到了区块链中，他添加的这笔奖励交易也可以被消费。

Jing, who participates in a mining pool, has set up his software to create new blocks that assign the reward to a pool address. From there, a share of the reward is distributed to Jing and other miners in proportion to the amount of work they contributed in the last round.
参与矿池的Jing设置了他的软件，使得构建新区块时会将奖励地址设为矿池的地址。
然后根据各自上一轮贡献的工作量，将所得的奖励分给Jing和其他矿工。

Alice’s transaction was picked up by the network and included in the pool of unverified transactions. Once validated by the mining software it was included in a new block, called a *candidate block*, generated by Jing’s mining pool. All the miners participating in that mining pool immediately start computing Proof-of-Work for the candidate block. Approximately five minutes after the transaction was first transmitted by Alice’s wallet, one of Jing’s ASIC miners found a solution for the candidate block and announced it to the network. Once other miners validated the winning block they started the race to generate the next block.
Alice的交易被网络收到后，放进未验证交易池中。
一旦被挖矿软件验证这个交易有效，这个交易就被包含在矿池生成的新区块（称为候选块）中。
参与该矿池的所有矿工立即开始计算候选块的工作量证明。
大约在Alice的钱包将这个交易发送出去五分钟后，Jing的ASIC矿机发现了新区块的正解，并将这个新区块发布到网络上后，一旦其它矿工验证了这个区块，它们就会立即投入到构建新区块的竞赛中。

Jing’s winning block became part of the blockchain as block #277316, containing 419 transactions, including Alice’s transaction. The block containing Alice’s transaction is counted as one "confirmation" of that transaction.
Jing的ASIC矿机发现了新区块的正解并将之发布为第277,316号区块，包含420个交易，包括Alice的交易。包含Alice交易的区块对这个交易来说是一次"确认"。

Tip: You can see the block that includes Alice’s transaction.
提示：你可以查看包含Alice交易的这个区块。
https://blockchain.info/block-height/277316

Approximately 19 minutes later, a new block, #277317, is mined by another miner. Because this new block is built on top of block #277316 that contained Alice’s transaction, it added even more computation to the blockchain, thereby strengthening the trust in those transactions. Each block mined on top of the one containing the transaction counts as an additional confirmation for Alice’s transaction. As the blocks pile on top of each other, it becomes exponentially harder to reverse the transaction, thereby making it more and more trusted by the network.
大约19分钟后，第277,317号新区块诞生在另一个挖矿节点。

因为这个新区块是在包含Alice交易的第277,316号区块的上层（栈），在这个区块的基础上增加了更多的计算，因此就加强了这个交易的可信度。
基于277,316号区块，每产生一个新区块，对这个交易来说就会增加了一次"确认"。
当区块一个个堆上来时，这个交易越来越难以推翻（指数级），因此它在网络中得到了更多信任。

In the diagram in Alice's transaction included in block #277316, we can see block #277316, which contains Alice's transaction. Below it are 277,316 blocks (including block #0), linked to each other in a chain of blocks (blockchain) all the way back to block #0, known as the *genesis block*. Over time, as the "height" in blocks increases, so does the computation difficulty for each block and the chain as a whole. The blocks mined after the one that contains Alice's transaction act as further assurance, as they pile on more computation in a longer and longer chain. By convention, any block with more than six confirmations is considered irrevocable, because it would require an immense amount of computation to invalidate and recalculate six blocks. We will examine the process of mining and the way it builds trust in more detail in [mining].
在图2-9中，包含Alice的交易的是第277,316号区块。
在它之下有277,316个区块（包括0号区块），像链子一样一个连一个（区块链），一直连到0号区块（创世区块）。
随着时间的流逝，这个区块链的高度也随之增长，每个区块和整个链的计算困难度也随之增加。
包含Alice的交易的区块后面形成的新区块，使得信任度进一步增加，因为他们叠加了更多的计算在这个越来越长的链上。
按照惯例，一个区块获得六次以上“确认”时，就被认为是不可撤销的了，因为要撤销和重建六个区块需要巨量的计算。
在第10章我们会详细描述挖矿和信任建立的过程。

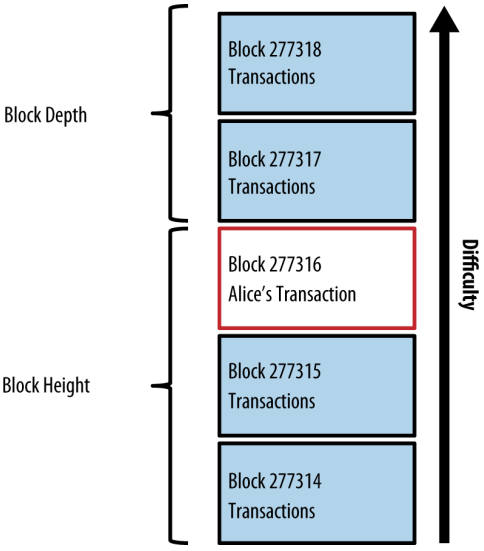

Figure 9. Alice's transaction included in block #277316

2.6 消费这笔交易

Now that Alice's transaction has been embedded in the blockchain as part of a block, it is part of the distributed ledger of bitcoin and visible to all bitcoin applications. Each bitcoin client can independently verify the transaction as valid and spendable. Full-node clients can track the source of the funds from the moment the bitcoin were first generated in a block, incrementally from transaction to transaction, until they reach Bob's address. Lightweight clients can do what is called a simplified payment verification (see [spv_nodes]) by confirming that the transaction is in the blockchain and has several blocks mined after it, thus providing assurance that the miners accepted it as valid.

既然Alice的这笔交易已经成为区块的一部分被加入到了区块链中，它就成为了整个分布式比特币账本的一部分，并对所有比特币客户端应用可见。每个比特币客户端都能独立验证这笔交易是有效且可消费的。全节点客户端可以追溯这笔的来源，从比特币第一次在区块中出现的时刻，按交易与交易间的关系顺藤摸瓜，直到Bob的交易地址。
轻量级客户端是一个简化的支付验证，通过确认这个交易在区块链中，且在它后面有几个新区块确认，从而保证矿工们认为它是有效的。。

Bob can now spend the output from this and other transactions. For example, Bob can pay a contractor or supplier by transferring value from Alice's coffee cup payment to these new owners. Most likely, Bob's bitcoin software will aggregate many small payments into a larger payment, perhaps concentrating all the day's bitcoin revenue into a single transaction. This would aggregate the various payments into a single output (and a single address). For a diagram of an aggregating transaction, see Transaction aggregating funds.
Bob现在可以花费此交易和其它交易的输出。例如，Bob可以把比特币转账给供应商以支付相应费用。大多数情况下，Bob用的比特币客户端会将多个小额支付聚合成一个大的支付，也许会将一整天的比特币收入聚合成一个交易。这样会将多个支付合入到咖啡店财务账户的一个单独地址。

As Bob spends the payments received from Alice and other customers, he extends the chain of transactions. Let's assume that Bob pays his web designer Gopesh in Bangalore for a new website page. Now the chain of transactions will look like Alice's transaction as part of a transaction chain from Joe to Gopesh.
当Bob花费从Alice和其他顾客那里赚得的比特币时，他就扩展了比特币的交易链。
而这个链会被加到整个区块链账本，使所有人知晓并信任。
我们假定Bob向Gopesh支付了一笔费用，那么区块交易链如图2-10所示。

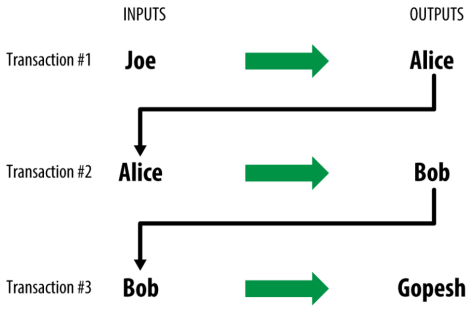

Figure 10. Alice's transaction as part of a transaction chain from Joe to Gopesh

In this chapter, we saw how transactions build a chain that moves value from owner to owner. We also tracked Alice's transaction, from the moment it was created in her wallet, through the bitcoin network and to the miners who recorded it on the blockchain. In the rest of this book, we will examine the specific technologies behind wallets, addresses, signatures, transactions, the network, and finally mining.
在本章中，我们看到了交易如何被构建为一个链，并将比特币从一个所有者转移给其他人。
我们还追踪了Alice的交易，从她的钱包创建这个交易的那刻起，通过比特币网络被矿工记录在区块链中。

在本书的其余部分，我们将研究钱包、地址、签名、交易、网络和挖矿等背后的具体技术。