第二章

2.1交易，块，挖矿和区块链

比特币系统与传统的银行和支付系统不同，是基于去中心化的信任。在比特币中，取代中央信任机构的是，信任是通过比特币系统中不同参与者的相互作用达成的。 在本章中，我们将通过较高层面跟踪比特币系统单笔交易，观察交易如何通过比特币分布式共识机制变得可信，被接受，并且最终记录在区块链，也就是所有交易的分布式账簿。随后的章节将深入探讨交易，网络和采矿背后的技术。

2.1.1比特币概述

如图2-1所示的概览图中，我们可以看到比特币系统由用户（用户通过密钥控制钱包）、交易（每一笔交易都会被广播到整个比特币网络）和矿工（通过竞争计算生成在每个节点达成共识的区块链，区块链是一个分布式的公共权威账簿， 包含了比特币网络发生的所有的交易）组成。

本章中的每个示例都基于在比特币网络上进行的实际交易，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。 在通过比特币网络跟踪交易到区块链时，我们将使用一个区块链接浏览器站点来显示每个步骤。 blockchain explorer是一个作为比特币搜索引擎运行的Web应用程序，它允许您搜索地址，交易和块，并查看它们之间的关系和资金流动。

\图2-1比特币网络概览

常见的区块链数据查询网站包括：

▷Bitcoin Block Explorer

▷BlockCypher Explorer▷blockchain.info

▷BitPay Insight

以上每一个查询网站都有搜索功能，可以通过地址，交易哈希值或区块号，搜索到在比特币网络和区块链中对应的数据。我们将给每个交易和区块例子提供一个链接，方便你做详细研究。

2.1.2买咖啡

在之前章节里，Alice是一名刚刚获得第一枚比特币的新用户。在“1.4.2 获取你的第一枚比特币 ”一节中，Alice和她的朋 友Joe会面时，用现金换取了比特币。由Joe产生的这笔交易使得Alice的钱包拥有了0.10比特币。现在Alice将第一次使用比特币在加利福尼亚州帕罗奥图的Bob咖啡店买一杯咖啡。

Bob咖啡店给他的销售网点系统新增加了一个比特币支付选项，价格单上列的是当地货币（美元）的售价，但在收银台，顾客可以选择用美元或比特币支付。此时，Alice点了杯 咖啡，然后Bob将交易键入到收银机，之后销售系统将按照当前市场汇率把美元总价转换为比特币，然后同时显示两种货币的价格：

总价:

$1.50 USD

0.015 BTC

Bob说到，“总共1.50美元，或0.015 BTC比特币”

Bob的自助销售系统还将自动创建一个包含付款请求的二维码。

与一个简单包含目的比特币地址的二维码不同，当前支付请求的是一个二维编码过的URL，它包含有一个目的地址，一笔支付金额，和一个像“Bob咖啡”这样的交易描述。这使比特币钱包应用在发送支付请求时，可以预先填好支付用的特定信息，给用户显示一种友好易懂的描述。你可以用比特币钱包应用扫描这个二维码来看Alice可能看到的信息。

图2-2支付请求二维码

提示尝试用你的钱包扫描这个，看看地址和金额，但不要发送货币。

根据BIP0021的定义，这个付款二维码包括的URL的意思是：

```
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用她的智能手机扫描了显示的条形码。，然后她按下发送键授权了这笔支付。在几秒钟时间内（大约与信用卡授权所需时间相同）Bob将会在收银台看到这笔交易，并完成交易。在接下来的章节中，我们将更详细地检视这笔交易，观察Alice的钱包是怎样构建交易，交易又是怎样在网络中广播、怎 样被验证，以及Bob在后续交易中怎样消费那笔钱。

注意从千分之一比特币(1毫比特币）到一亿分之一比特币（1聪比特币），比特币网络可以处理任意小额交易。在本书 中，我们将用“比特币”这个术语来表示任意数量的比特币货币，从最小单元（1聪）到可被挖出的所有比特币总数 （21,000,000）。你可以像例1那样使用区块资源管理器站点来检查Alice与Bob's Cafe的交易:

例1. 查看Alice的交易

点击查看Alice的交易

2.2 比特币交易

简单来说，交易告知全网：比特币的持有者已授权把比特币转帐给其他人。而新持有者能够再次授权，转移给该比特币所有权链中的其他人，产生另一笔交易来花掉这些比特币，后面的持有者在花费比特币也是用类似的方式。

2.2.1交易输入输出

交易就像复式记账法账簿中的行。简单来说，每一笔交易包含一个或多个“输入”，输入是针对一个比特币账号的负债。 这笔交易的另一面，有一个或多个“输出”，被当成信用积分记入到比特币账户中。这些输入和输出的总额（负债和信用）不需要相等。相反，当输出累加略少于输入量时，两者的差额就代表了一笔隐含的“矿工费”，这也是将交易放进账簿的矿工所收集到的一笔小额支付。如图2-3描述的是一笔作为记账簿记录的比特币交易。交易也包含了每一笔被转移的比特币（输入）的所有权证明，它以所有者的数字签名形式存在，并可以被任何人独立验证。在比特币术语中，“消费”指的是签署一笔交易：转移一笔以前交易的比特币给以比特币地址所标识的新所有者。

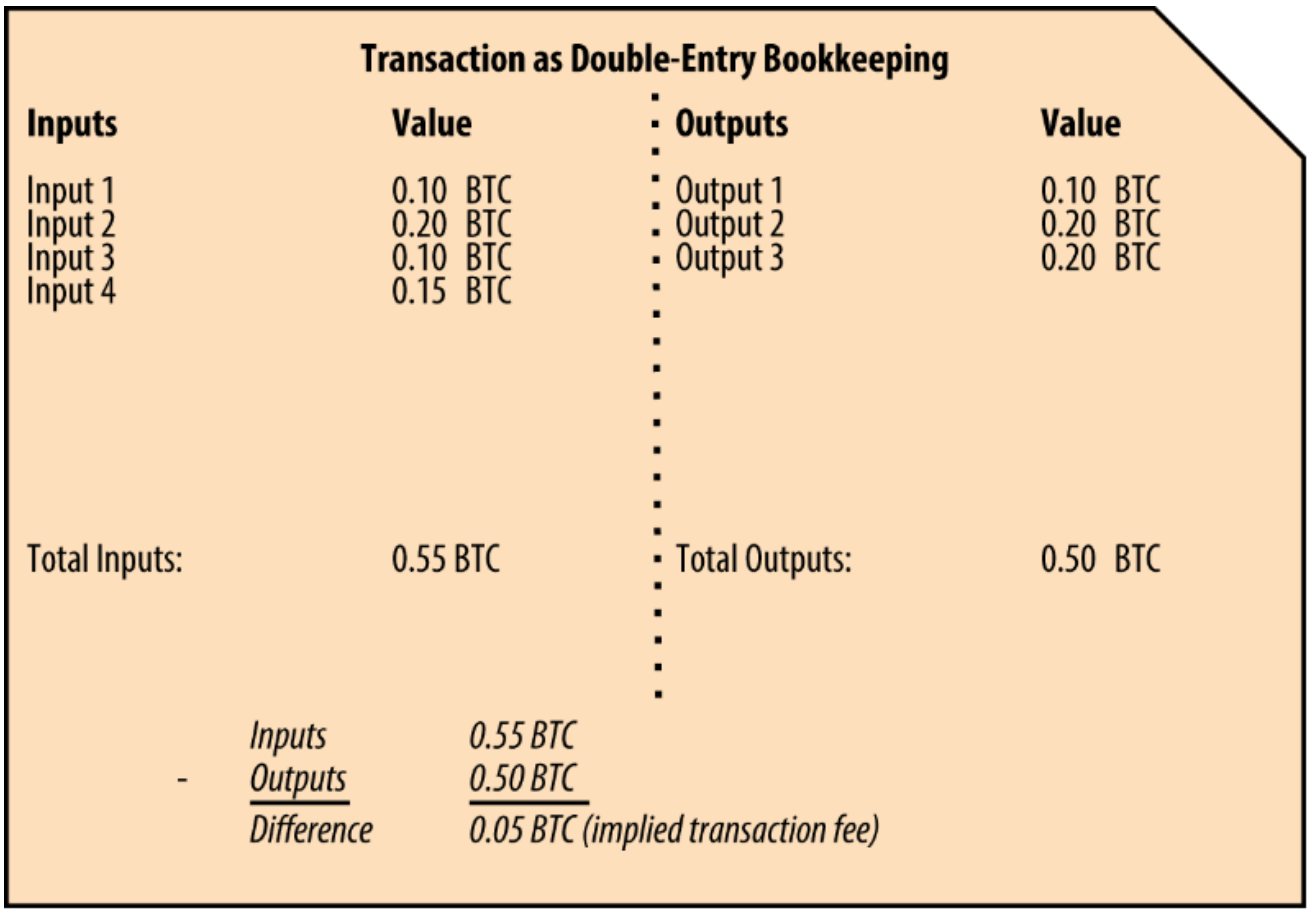

图2-3交易就像复式记账

2.2.3交易链

Alice支付Bob咖啡时使用一笔之前的交易作为输入。在以前的章节中，Alice从她朋友Joe那里用现金换了点比特币。那笔交易创建了一些被Alice的密钥锁定的比特币。在她支付Bob咖啡店的新交易中使用了之前的交易作为输入，并以支付咖啡和找零作为新的输出。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的密钥提供了解锁之前交易输出的签名，因此向比特币网络证明她拥有这笔钱。她将买咖啡的这笔支付附加到Bob的地址上，实现“阻止”那笔输出，明确指明要求是Bob签名才能消费这笔钱。这就描述了在Alice和Bob之间钱的转移。下图展示了从Joe到Alice再到Bob的交易链。

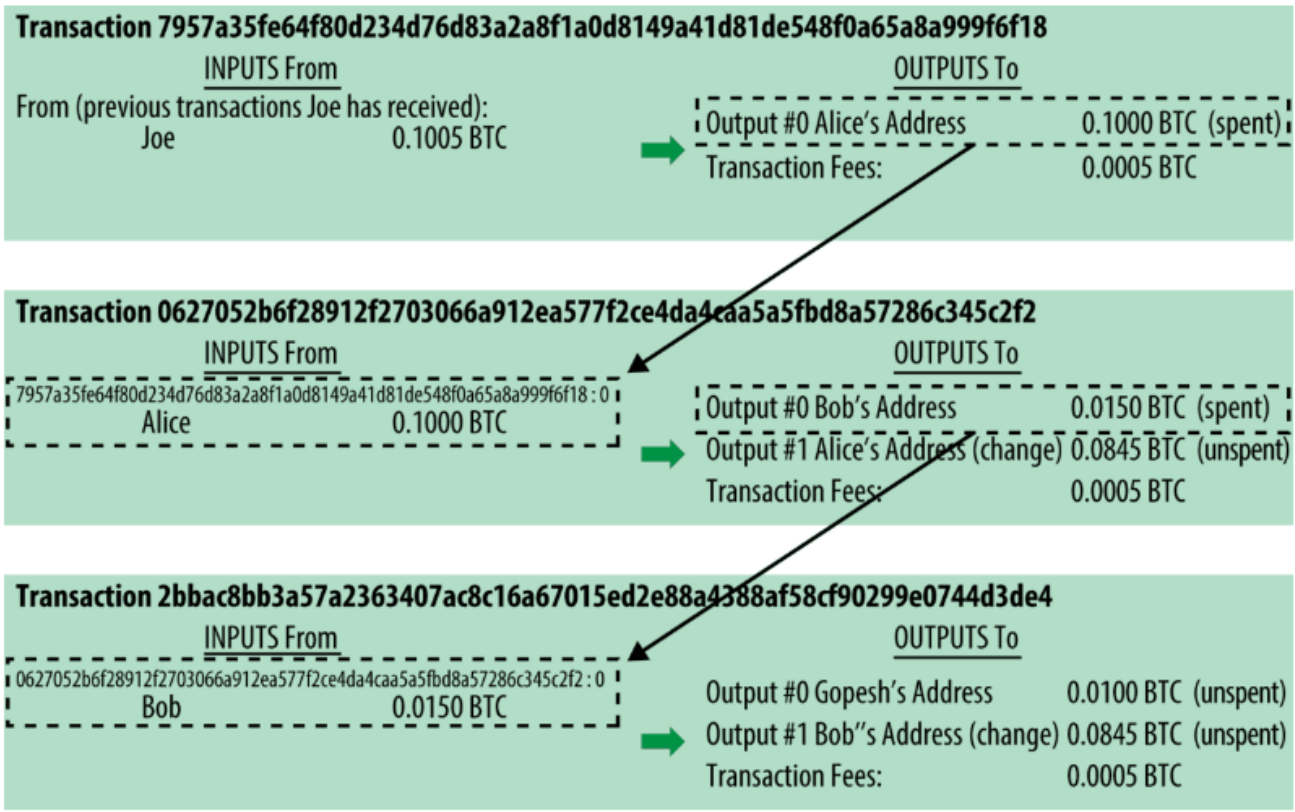

图2-5交易链中，一笔交易输出就是另一笔交易的输入

2.2.4找零

许多比特币交易都会包括新所有者的地址（买方地址）和当前所有者的地址（称为找零地址）的输出。这是因为交易输入，就像纸币那样能够，不能再分割。如果您在商店购买了5美元的商品，但是使用20美元的美金来支付商品，您预计会收到15美元的找零。相同的概念适用于比特币交易输入。如果您购买了一个价格为5比特币但只能使用20比特币输入的商品，那么您可以将5个比特币的一个输出发送给商店所有者，并将一个15比特币的输出返回给您自己作为找零（减去任何适用的交易费用）。重要的是，找零地址不必与输入时提供的地址相同，出于隐私的原因，通常是所有者钱包中的新地址。

不同的钱包可以在汇总输入以进行用户请求的付款时使用不同的策略。它们可能会聚合许多小输入，或者使用等于或大于所需付款的输入。除非钱包可以以这样的方式汇总输入，以便将所需付款与交易费用完全匹配，否则钱包将需要产生一些找零。这与人们如何处理现金非常相似。如果你总是在你的钱包支付时使用最大的面额，你会最终得到一个充满零钱的钱包。如果你只使用零钱，你最终会换来整钱。人们总是在潜意识中在这两个极端之间找到平衡，而比特币钱包开发商也力图实现这种平衡。总的来讲，交易是将钱从交易输入移至输出。输入是指钱币的来源，通常是之前一笔交易的输出。交易输出将约定金额发送到新的所有者的比特币地址，并将找零输出返回原来原来所有者。 一笔交易的输出可以被当做另一笔新交易的输入，这样随着钱从一个地址被移动到另一个地址的同时形成了一条所有权链（如图2-4）。

2.2.5 常见的交易形式

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给支付者的“找零”。一般交易有一个输入和两个输出，如图2-5所示:

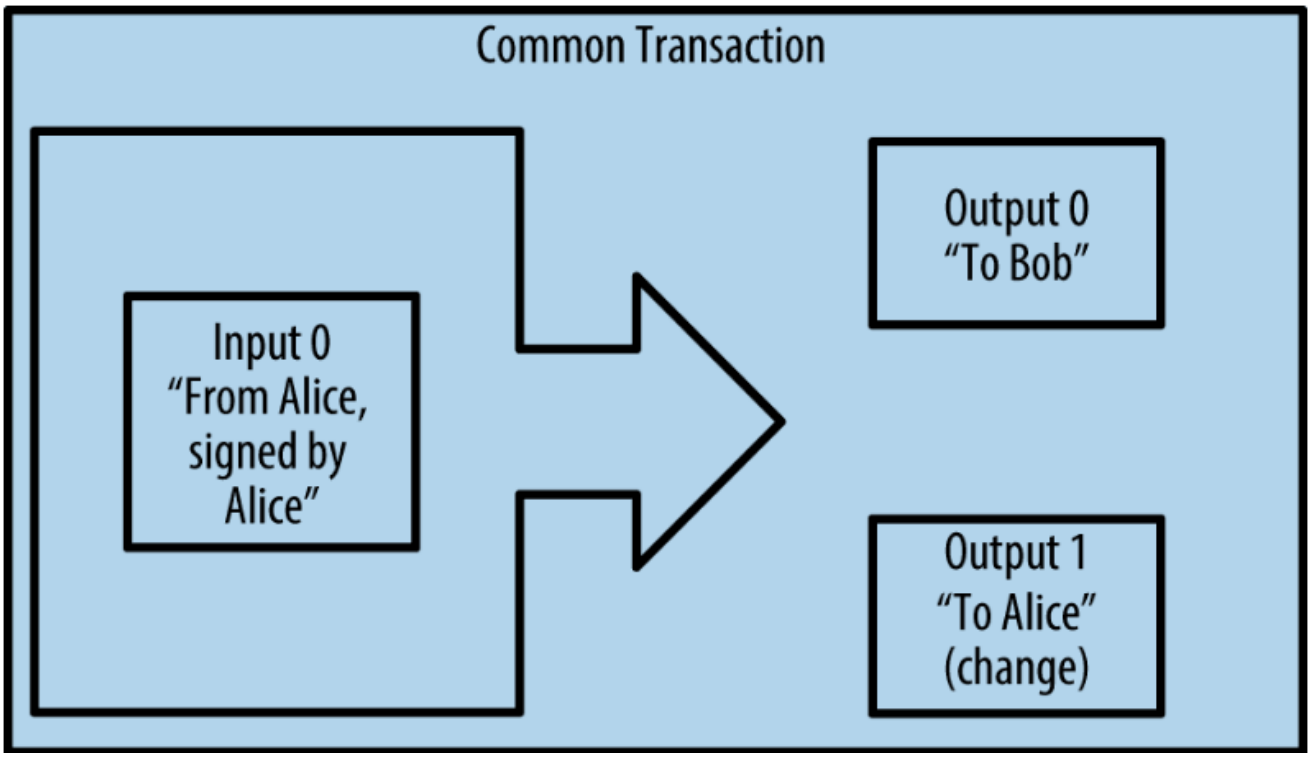

图2-5最普通的交易

另一种常见的交易形式是集合多个输入到一个输出（如图2-6）的模式。这相当于现实生活中将很多硬币和纸币零钱兑换为一个大额面钞。像这样的交易有时由钱包应用产生来清理许多在支付过程收到的小数额的找零。

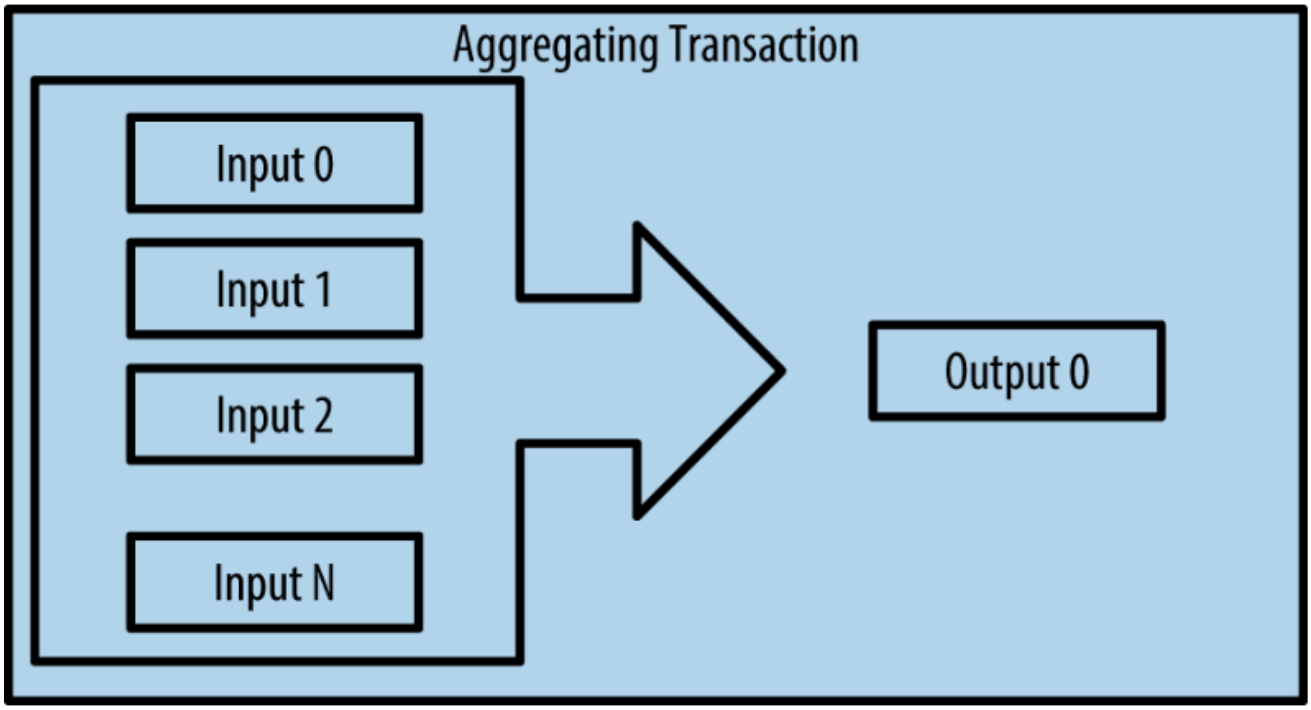

图2-6打包资金的交易

最后，另一种在比特币账簿中常见的交易形式是将一个输入分配给多个输出，即多个接收者（如图2-7）的交易。这类交易有时被商业实体用作分配资金，例如给多个雇员发工资的情形。

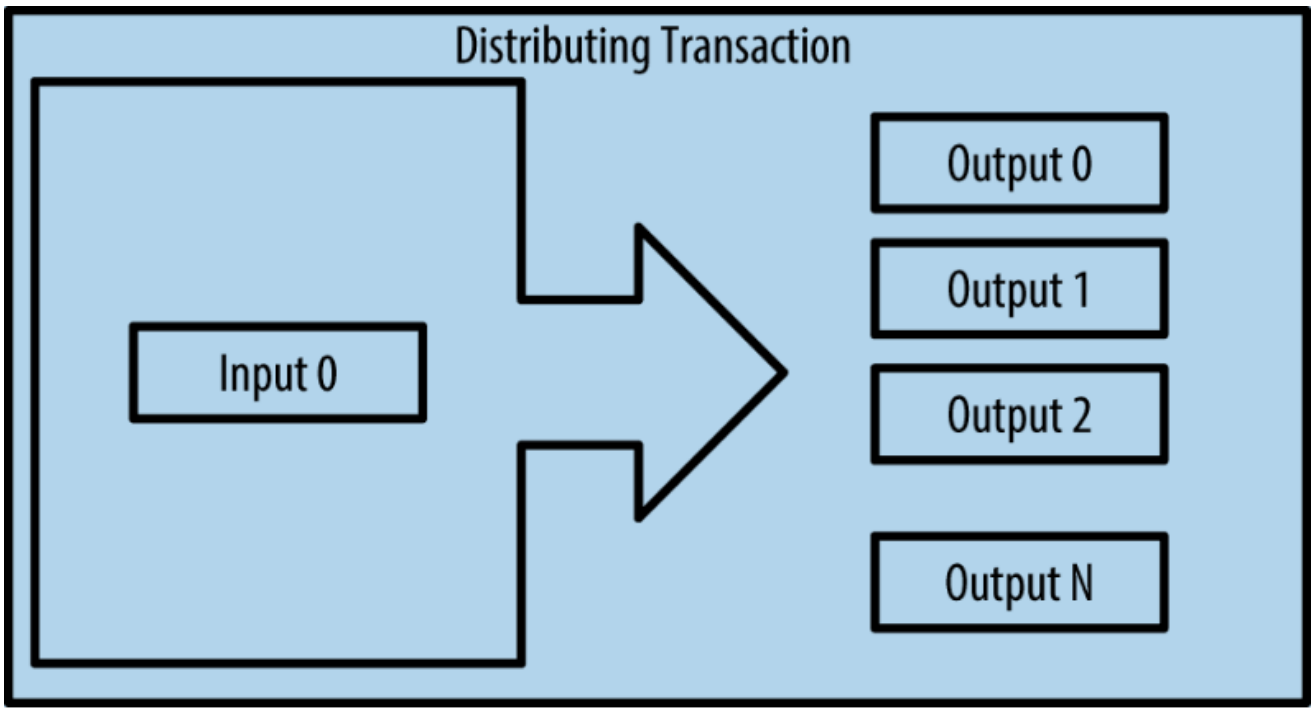

图2-7分散资金的交易

2.3 交易的构建

Alice的钱包应用知道如何选取合适的输入和输出以建立Alice所希望的交易。Alice只需要指定目标地址和金额，其余的细节钱包应用会在后台自动完成。很重要的一点是，钱包应用甚至可以在完全离线时建立交易。就像在家里写张支票， 之后放到信封发给银行一样，比特币交易建立和签名时不用连接比特币网络。只有在执行交易时才需要将交易发送到网络。

2.3.1 获取正确的输入

Alice的钱包应用首先要找到一些足够支付给Bob所需金额的输入。大多数钱包应用跟踪着钱包中某个地址的所有可用输出。因此Alice的钱包会包含她用现金从Joe那里购买的比特币的交易输出副本（参见 在“获取你的第一枚比特币”一节）。完整客户端含有整个区块链中所有交易的所有未消费输出副本。这使得钱包既能拿这些输出构建交易，又能在收到新交易时很快地验证其输入是否正确。然而，完整客户端占太大的硬盘空间，所以大多数钱包使用轻量级的客户端，只保存用户自己的未消费输出。

如果钱包客户端没有某一未消费交易输出，它可以通过不同的服务者提供的各种API或完整索引节点的JSON PRC API从比特币网络中拿到这一交易信息。例子2-1展示了用HTTP GET命令对一个特定URL建立了一个API的请求。这个URL会返回一个地址的所有未消费交易输出，以提供给需要这些信息的任何应用作为建立新交易的输入而进行消费。 我们用一个简单的HTTP命令行客户端 cURL来获得这个响应数据。

例2-1 查找Alice的比特币地址所有的未消费的输出

```
$ 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
        }

    ]
}
```

例2-2的响应数据显示了在Alice的地址 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK 上面有一个未消费输出（还未被兑换）。这个响应包含一个交易的引用。而从Joe那里转过来的未消费输入就包含在这个交易里面，它的价值是一千万聪 （satoshi），即 0.10比特币。通过这个信息，Alice的钱包应用就可以创建新的交易将钱转账到新地址。

提示点击这里 查看Joe和Alice间的交易信息。

如你所见，Alice的钱包在单个未消费的输出中有足够的比特币支付一杯咖啡。假如不够的话，Alice的钱包应用就不得不搜寻一些小的未消费输出，像是从一个存钱罐里找硬币一样，直到找到足够支付咖啡的数量。在两种情境下，可能都需要找回零钱，而这些找零也会是钱包所创建的交易的输出组成部分。我们会在下一节会有所描述。

2.3.2 创建交易输出

交易的输出会被创建成为一个包含这笔数额的脚本的形式，只能被引入这个脚本的一个解答后才能兑换。简单点说就 是，Alice的交易输出会包含一个脚本，这个脚本说 “这个输出谁能拿出一个签名和Bob的公开地址匹配上，就支付给谁”。因为只有Bob的钱包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兑换这笔输出。因此Alice 会需要Bob的签名来包装一个输出。

这个交易还会包含第二个输出。因为Alice的金额是0.10比特币的输出形式，对0.015 比特币一杯的咖啡来说太多了，需要找Alice 0.085比特币的零钱。Alice钱包创建给她的零钱的支付就在付给Bob的同一个交易里面。可以说，Alice的钱包将她的金额分成了两个支付：一个给Bob，一个给自己。她可以在以后的交易里消费这笔零钱输出。但这并不意味着可以用作用户或应用程序的生产钱包。 建议应用

最后，为了让这笔交易尽快地被网络处理，Alice的钱包会多付一小笔费用。这个不是明显地包含在交易中的；而是通过输入和输出的差值所隐含的。如果Alice创建找零时只找 0.0845比特币，而不是 0.085比特币的话，这里就有剩下 0.0005比特币（50万聪） 。因为加起来小于 0.10，所以这个 0.10 比特币的输入就没有被完整的消费了。这个差值会就被矿工当作交易费放到区块的交易里，最终放进区块链帐薄中。

这个交易的结果信息可以用区块链数据查询站点看到，如图2-8所示。

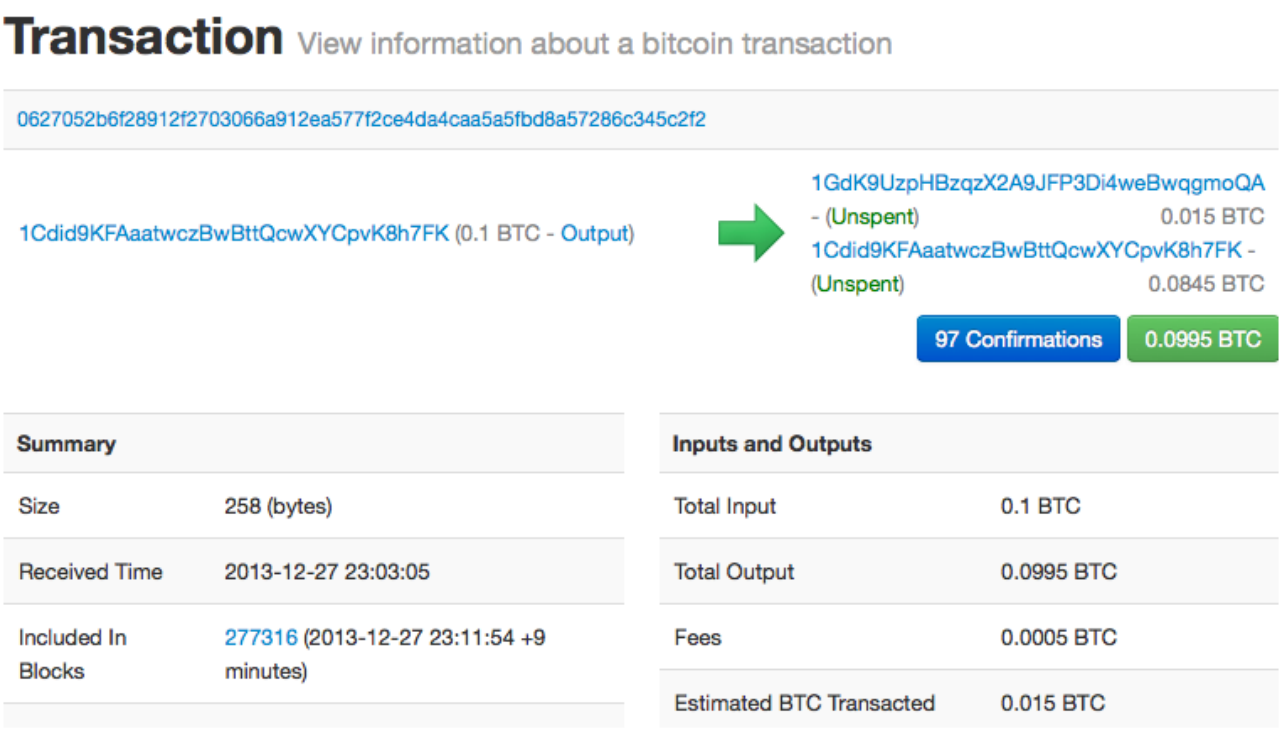

图2-8 Alice和Bob咖啡店的交易

2.3.3 将交易放到总账簿中

这个被Alice钱包应用创建的交易大小为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中以成为分布式账簿（区块链）的一部分。在下一节里，我们来看下一个交易如何成为新区块的一部分， 以及区块是如何被挖矿构建的。最后，我们会看看新区块被加进区块链后，是如何随更多区块的添加而增加可信度的。

2.3.3.1 交易的传送

因为这个交易包含处理所需的所有信息，所以这个交易是被如何或从哪里传送到比特币网络的就无所谓了。比特币网络是由参与的比特币客户端联接几个其他比特币客户端组成的P2P网络。比特币网络的目的是将交易和区块传播给所有参与者。

2.3.3.2 如何传播

“说着”比特币协议，从而实现参与比特币网络的任何系统（例如服务器，桌面应用程序或钱包）都称为比特币节点。Alice的钱包应用可以发送新的交易给其它任意一个已联接到互联网的比特币客户端，不论其是由有线网、WiFi、还是通过手机联接的。她的钱包不必直接连着Bob的比特币钱包，且她不必使用咖啡厅提供的网络联网，虽然这两者都是可能的。任何比特币网络节点（其它客户端）收到一个之前没见过的有效交易时会立刻将它转发给联接到自身的其它节点。 因此，这个交易迅速地从P2P网络中传播开来，几秒内就能到达大多数节点。

2.3.3.3 Bob的视角

如果Bob的比特币钱包应用是直接连接Alice的钱包应用的话，Bob的钱包应用也许就是第一个收到这个交易的节点。然 而，即使Alice的交易是从通过其它节点发过来的，一样可以在几秒钟内到达Bob钱包应用这里。Bob的钱包会立即确认 Alice的交易是一个收入支付，因为它包含能用Bob的私钥兑换的输出。Bob的钱包应用也能够独立地用之前未消费输入来确认这个交易是正确构建的，并且由于包含足够交易费会被下一个区块包含进去。这时Bob只需冒很小的风险，因为这个交易会很快被加到区块且被确认。

提示一个对比特币交易的常见误解是它们必须要等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。一个商家可以免确认来接受比特币小额支付。这样做的风险不比接受一个不是用有效身份证领取或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

这个交易现在在比特币网络上传播开来。但只有被一个称为挖矿的过程验证且加到一个区块中之后，这个交易才会成为 这个共享账簿（区块链）的一部分。关于挖矿的详细描述请见第10章。比特币系统的信任是建立在计算的基础上的。交易被包在一起放进区块中时需要极大的计算量来证明，但只需少量计算就能验证它们已被证明。

挖矿在比特币系统中有两个重要作用：

▷ 挖矿节点通过参考比特币的共识规则验证所有交易。 因此，挖矿通过拒绝无效或畸形交易来提供比特币交易的安全性。

▷ 挖矿在构建区块时会创造新的比特币，和一个中央银行印发新的纸币很类似。每个区块创造的比特币数量是固定的， 随时间会渐渐减少。

挖矿在成本和报酬之间取得了良好的平衡。 挖矿采用电力来解决数学问题。 一个成功的矿工将以新的比特币和交易费的形式获取奖励。 但是，只有矿工正确验证了所有的交易，才能获得奖励，才能达到协商一致的规则。 这种微妙的平衡为没有中央权力机构的比特币提供安全保障。

描述挖矿的一个好方法是将之类比为一个巨大的多人数独谜题游戏。一旦有人发现正解之后，这个数独游戏会自动调整难度以使游戏每次需要大约10分钟解决。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，就会花费非常长的时间来解决。这个数独游戏的困难度可以通过改变其大小（更多或更少行列）来调整，但即使它非常大时验证它也是相当容易的。而比特币中的 "谜题" 是基于哈希加密算法的，其展现了相似的特性：非对称地，它解起来困难而验证很容易，并且它的困难度可以调整。

在 “比特币的应用、用户和他们的故事”一节中，我们提到了一个叫Jing的在上海学计算机工程的学生。Jing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的交易寻找正解的全球竞赛。为寻找这个解，也被称为工作量证明，整个网络需要具有每秒亿万次哈希计算的能力。这个工作量证明算法指的用SHA256加密算法不断地对区块头和一个随机数字进行哈希计算，直到出现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会将此区块发布到区块链中。

Jing从2010年开始挖矿，当时他使用一个非常快的桌面电脑来为新区块寻找正解。随着更多的矿工加入比特币网络中， 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 独享图像处理单元芯片（即显卡GPU）。在写这本书的时候，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的公司同时加入了一个类似彩票奖池的、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，通过收益获得一些收入。

2.5 区块中的挖矿交易记录

新交易不断地从用户钱包和应用流入比特币网络。当比特币网络上的节点看到这些交易时，会先将它们放到各自节点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， 会将这些交易从这个交易池中拿出来放到这个新区块中，然后通过尝试解决一个非常困难的问题（也叫工作量证明）以证明这个新区块的合法性。挖矿过程的细节会在“挖矿简介”一节中详加描述。

这些交易被加进新区块时，以交易费用高的优先以及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，会马上开始下一个新区块的挖掘工作。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，并开始给它计算工作量证明。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（当前每区块为12.5比特币）作为报酬支付到他自己的比特币地址，再加上块中所有交易的交易费用的总和作为自己的报酬。如果他找到了使得新区块有效的解法，他就会得到这笔报酬，因为这个新区块被加入到了总区块链中，他添加的这笔报酬交易也会变成可消费的。 参与矿池的Jing设置了他的软件，使得构建新区块时会将报酬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报酬分给Jing和其他参与矿池挖矿的矿工。

Alice的交易被网络拿到后放进未验证交易池中。一旦被挖矿软件验证，它就被包含在由Jing的采矿池生成的新块（称为候选块）中。 参与该采矿池的所有矿工立即开始计算候选块的工作证明。大约 在Alice的钱包第一次将这个交易发送出来五分钟后，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，一旦被其它矿机验证，它们就会立即投身到构建新区块的竞赛中。

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算一次"确认"。

提示你可以查看包含Alice交易记录的这个区块的信息。

大约19分钟后，第277,317号新区块诞生在另一个挖矿节点中。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，因此就加强了这些交易的可信度。基于这个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，这个交易变得指数级地越来越难被推翻，因此它在网络中得到更多信任。

在图2-9中，我们可以看到包含Alice的交易的第277,316号区块。在它之下有377,361个区块（包括0号区块），像链子 一样一个连着一个（区块链），一直连到0号区块，即创世区块。随着时间变长，这个区块链的高度也随之增长，每个区块和整个链的计算复杂度也随之增加。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子上。按惯例来说，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。

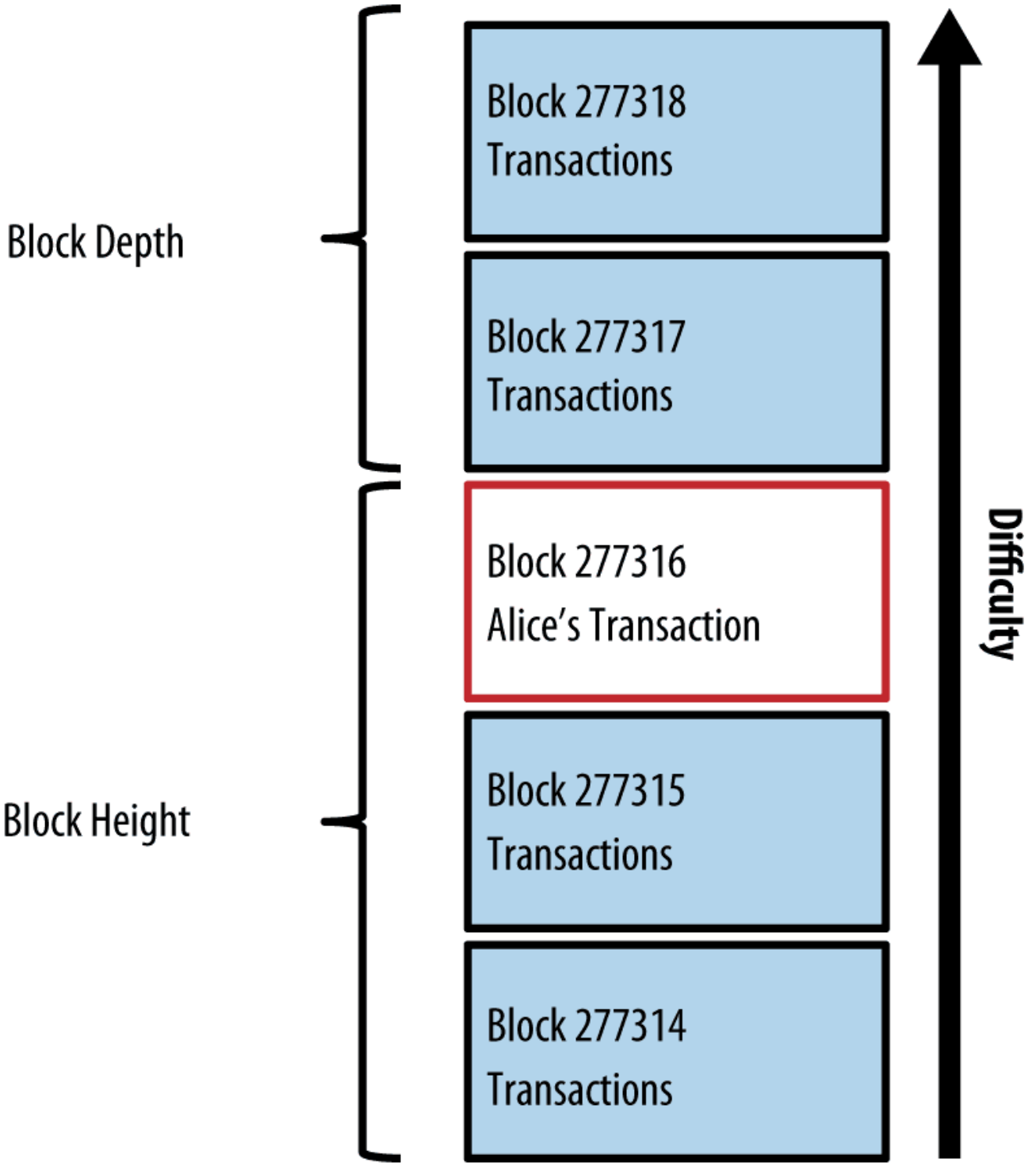

图2-9Alice的交易包括在区块277316

2.6 消费这笔交易

既然Alice的这笔交易已经成为区块的一部分被嵌入到了区块链中，它就成为了整个分布式比特币账簿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地验证这笔交易是有效且可消费的。全节点客户端可以追溯钱款的来源，从第一次有比特币在区块里生成的那一刻开始，按交易与交易间的关系顺藤摸瓜，直到Bob的交易地址。轻量级客户端通过确认一个交易在区块链中且在它后面有几个新区块来确认一个支付的合法性。这种方式叫做简易支付验证（参 见“简易支付验证（SPV）节点”）。

Bob现在可以将此交易和其它交易的结果信息作为输入，创建新的所有权为其他人的交易。这样就实现了对此交易的消费。举个例子，Bob可以用Alice支付咖啡的比特币转账给承包商或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成到咖啡店财务账户的一个单独地址。图2-10为交易集合示例。

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条。而这个链条会被加到整个区块链账簿，使所有人知晓并信任。我们假定Bob向在邦加罗尔的网站设计师Gopesh支付一个新网页的设计费用。那么区块交易链如图2-10所示。

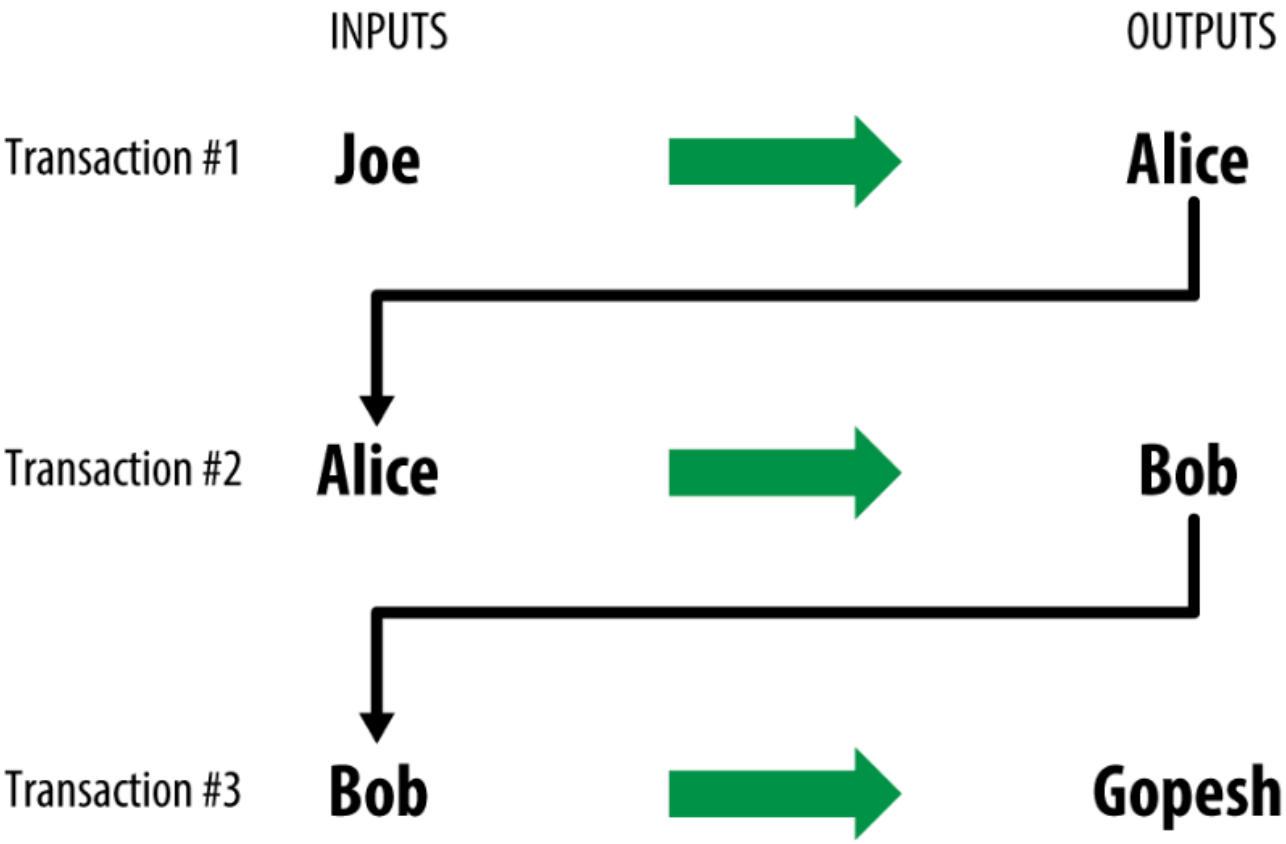

图2-10Alice的交易成为 Joe 和 Gopesh交易的一部分

在本章中，我们看到了交易如何被构建为一个链，并将价值从一个所有者转移到所有者。 我们还追踪了Alice的交易，从她的钱包中创建的那一刻起，通过比特币网络被矿工记录在区块链。 在本书的其余部分，我们将研究钱包，地址，签名，交易，网络和最终挖矿等背后的具体技术。