فصل

۲

بیت‌کوین چگونه کار می‌کند

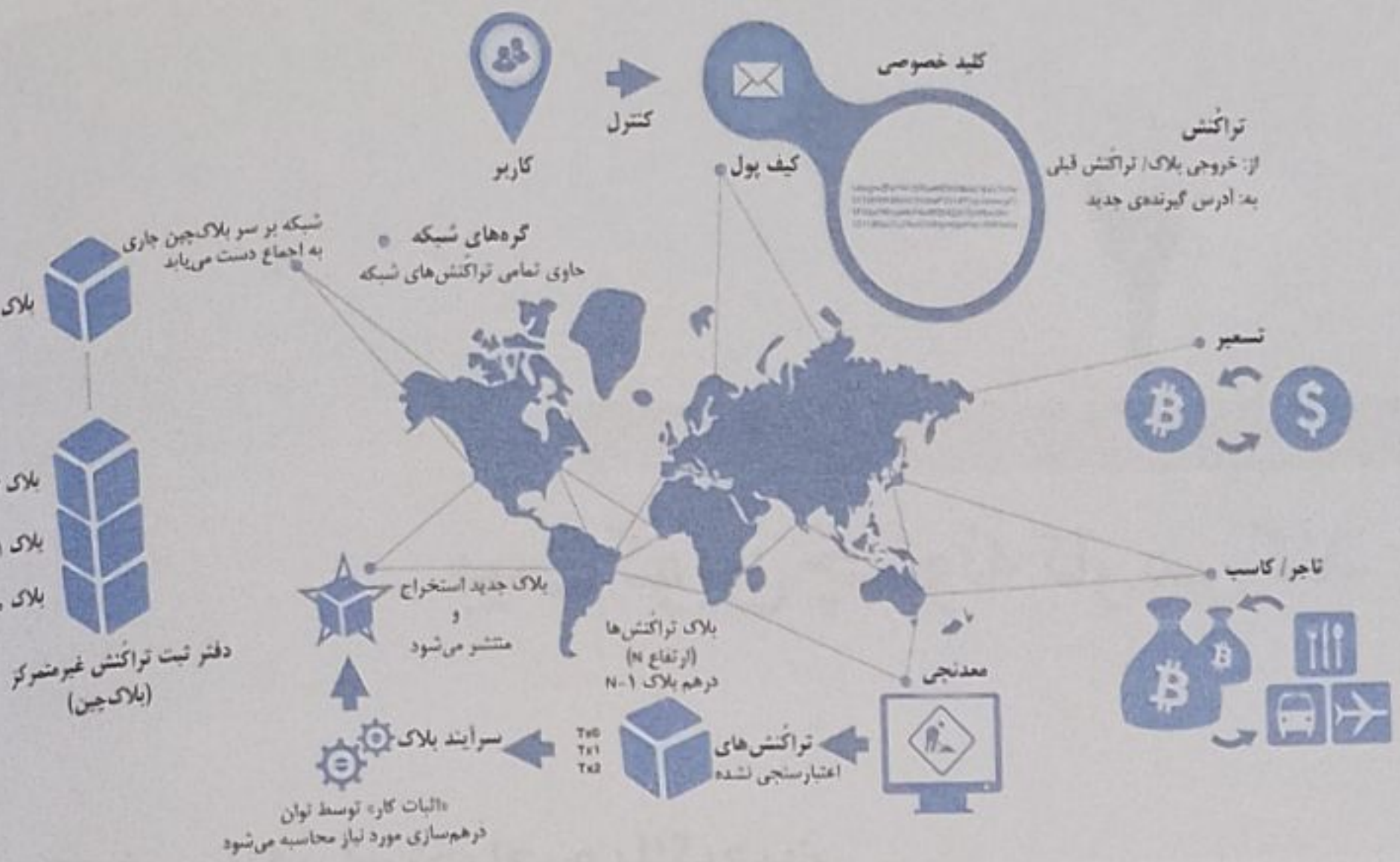
تراکُنش، بلاک، استخراج، و بلاک‌چین

بر خلاف سیستم‌های بانکداری و پرداخت سنتی، سیستم بیت‌کوین بر اساس *اعتماد غیرمتمرکز* بنا شده است. در بیت‌کوین به جای یک مرجع مورد اعتماد مرکزی، اعتماد به عنوان یک خاصیت برآمده از برهم‌کُنش بین اعضای مختلف شبکه ظاهر می‌شود. در این فصل با پیگیری مسیر حرکت یک تراکُنش در سیستم بیت‌کوین و دیدن این که چگونه این تراکُنش به وسیله‌ی ساز و کار *اجماع غیرمتمرکز* پذیرفته شده و مورد اعتماد قرار می‌گیرد و سرانجام در بلاک‌چین، دفتر کل غیرمتمرکز تراکُنش‌ها، ثبت می‌شود، با ساز و کار بیت‌کوین آشنا می‌شویم. در فصل‌های آینده به تشریح فناوری‌های به کار رفته در تراکُنش‌ها، شبکه‌ی بیت‌کوین، و استخراج آن خواهیم پرداخت.

مروری بر بیت‌کوین

نمودار کلی سیستم بیت‌کوین را در شکل ۲-۱ مشاهده می‌کنید؛ همان طور که در این نمودار می‌بینید، سیستم بیت‌کوین از چند بخش اصلی تشکیل شده است: کیف‌پول‌هایی که حاوی آدرس‌ها و کلیدهای خصوصی هستند، تراکُنش‌هایی که در سرتاسر شبکه منتشر می‌شوند، معدنچیانی که (از طریق رقابت در محاسبه) بلاک‌چین اجماع را تولید می‌کنند، و بلاک‌چینی که دفتر کل مرجع تمامی تراکُنش‌های شبکه است.

تمامی مثال‌های این فصل بر اساس تراکُنش‌های واقعی هستند که در شبکه‌ی بیت‌کوین اتفاق افتاده‌اند، و برهم‌کُنش بین کاربران (جو، آلیس، باب و گوپش) و انتقال وجه از یک کیف‌پول به کیف‌پول دیگر را شبیه‌سازی می‌کنند. برای دنبال کردن مسیر حرکت یک تراکُنش در شبکه‌ی بیت‌کوین برای ورود به بلاک‌چین، از یک سایت کاوشگر بلاک‌چین (blockchain explorer) برای به تصویر کشیدن مراحل مختلف این مسیر استفاده خواهیم کرد. کاوشگر بلاک‌چین یک برنامه‌ی کاربردی وب است که به عنوان موتور جستجوی بیت‌کوین عمل می‌کند و اجازه می‌دهد آدرس‌ها، تراکُنش‌ها و بلاک‌ها را جستجو کنید و روابط و گردش کار بین آنها را ببینید. از میان رایج‌ترین کاوشگرهای بلاک‌چین می‌توان به کاوشگرهای زیر اشاره کرد:



شکل ۲-۱ نمودار کلی بیت‌کوین.

- کاوشگر Bitcoin Block (به آدرس https://blockexplorer.com)
- کاوشگر BlockCypher (به آدرس https://live.blockcypher.com)
- کاوشگر blockchain.info (به آدرس https://blockchain.info)
- کاوشگر BitPay Insight (به آدرس https://insight.bitpay.com)

همه‌ی این کاوشگرها می‌توانند یک آدرس بیت‌کوین، دَرهم تراکُنش، شماره‌ی بلاک یا دَرهم آن را گرفته و اطلاعات متناظر با آن را از شبکه‌ی بیت‌کوین استخراج کنند. به ازای هر تراکُنش یا بلاک که در این مثال‌ها خواهید دید، URL آن را هم داده‌ایم تا خودتان بتوانید جزئیات آن را سر فرصت و با دقت بیشتر بررسی کنید.

خرید یک فنجان قهوه

در فصل قبل با آلیس آشنا شدیم که به تازگی وارد دنیای بیت‌کوین شده و موفق شد اولین بیت‌کوین خود را به دست آورد. دیدیم که آلیس برای به دست آوردن این بیت‌کوین به یکی از دوستان خود به نام جو پول نقد پرداخت کرد. تراکُنشی که جو ایجاد کرد، باعث شد تا ۰٫۱۰ BTC (یک‌دهم بیت‌کوین) به کیف‌پول آلیس واریز شود. اکنون آلیس می‌خواهد با این بیت‌کوین اولین خرید خود را انجام دهد و از مغازه‌ی باب (که در فصل قبل با او هم آشنا شدید) یک فنجان قهوه بخرد.

قهوه‌خانه‌ی باب به تازگی بیت‌کوین را هم به گزینه‌های سیستم نقطه‌ی-فروش (pos) خود اضافه کرده است و بیت‌کوین را به عنوان «پول» قبول می‌کند. در قهوه‌خانه‌ی باب قیمت‌ها بر اساس دلار آمریکا تعیین شده‌اند، ولی صندوق آن بیت‌کوین هم می‌پذیرد. وقتی آلیس یک فنجان قهوه سفارش می‌دهد، باب مثل همیشه برای آن صورتحساب صادر می‌کند، ولی این بار در صورتحساب مشتری دو قیمت جداگانه (یکی بر حسب دلار آمریکا، و دیگری معادل آن به بیت‌کوین بر اساس نرخ فعلی بازار) دیده می‌شود:

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

شکل ۲-۲ کُد QR درخواست پرداخت.

باب با این صورتحساب اعلام می‌کند، «یک فنجان قهوه، یک و نیم دلار، یا ۱۵ میلی‌بیت‌کوین.» دستگاه pos باب همچنین به طور خودکار کُد QR متناظر با این *درخواست پرداخت* را نیز تولید می‌کند؛ شکل ۲-۲ را ببینید.

بر خلاف کُد QR آدرس بیت‌کوین (که در فصل قبل دیدیم)، کُد QR درخواست پرداخت حاوی یک URL است که اطلاعات آدرس مقصد (گیرنده‌ی بیت‌کوین)، مقدار پرداخت، و یک عبارت توصیفی (مثل «قهوه‌خانه‌ی باب») را در خود جای داده است. این کُد QR به برنامه‌ی کیف‌پول بیت‌کوین اجازه می‌دهد تا اطلاعات لازم برای انجام این پرداخت و همچنین توصیفی کاربر-پسند از آن تراکُنش را در اختیار داشته باشد. برای انجام این پرداخت با بیت‌کوین، فقط کافی است آلیس کُد QR فوق را با برنامه‌ی کیف‌پول خود اسکن کند. شما هم می‌توانید این کُد QR را در گوشی خود اسکن کنید و اطلاعات موجود در آن را ببینید:

```
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"
```

این کُد QR را در گوشی خود اسکن کنید و آدرس مقصد و مقدار پرداخت آن را ببینید، ولی دکمه‌ی **Send** را نزنید!

آلیس این کُد QR را با گوشی هوشمند خود اسکن کرده و بعد از دیدن اطلاعات پرداخت، با زدن دکمه‌ی Send اجازه‌ی پرداخت آن را صادر می‌کند. چند ثانیه بعد (حدوداً همان مقداری که برای پرداخت با کارت بانکی باید صبر کنید)، باب این تراکُنش را در صندوق خود می‌بیند و تراکُنش به پایان می‌رسد.

در ادامه این تراکُنش را با جزئیات بیشتر بررسی می‌کنیم، و خواهید دید که کیف‌پول آلیس چگونه این تراکُنش را تولید می‌کند، این تراکُنش چگونه در شبکه‌ی بیت‌کوین منتشر می‌شود، چگونه اعتبارسنجی می‌شود، و سرانجام باب چگونه می‌تواند مقدار دریافتی را در تراکُنش‌های بعدی خرج کند.

نکته

در شبکه‌ی بیت‌کوین، تراکُنش‌ها می‌توانند کسری از بیت‌کوین، تا یک ساتوشی یا ۰٫۰۰۰۰۰۰۰۱ بیت‌کوین باشند. در این کتاب از کلمه‌ی «بیت‌کوین» برای اشاره به هر مقدار از این پول، از ۱ ساتوشی (کوچک‌ترین واحد) گرفته تا ۲۱ میلیون بیت‌کوین (کل پولی که می‌توان از این شبکه استخراج کرد)، استفاده خواهیم کرد.

پرداخت آلیس به باب را می‌توانید با استفاده از یک کاوشگر بلاک‌چین نیز بررسی کنید؛ مثال ۲-۱ را ببینید.

مثال ۲-۱ نمایش تراکُنش آلیس در کاوشگر blockexplorer.com

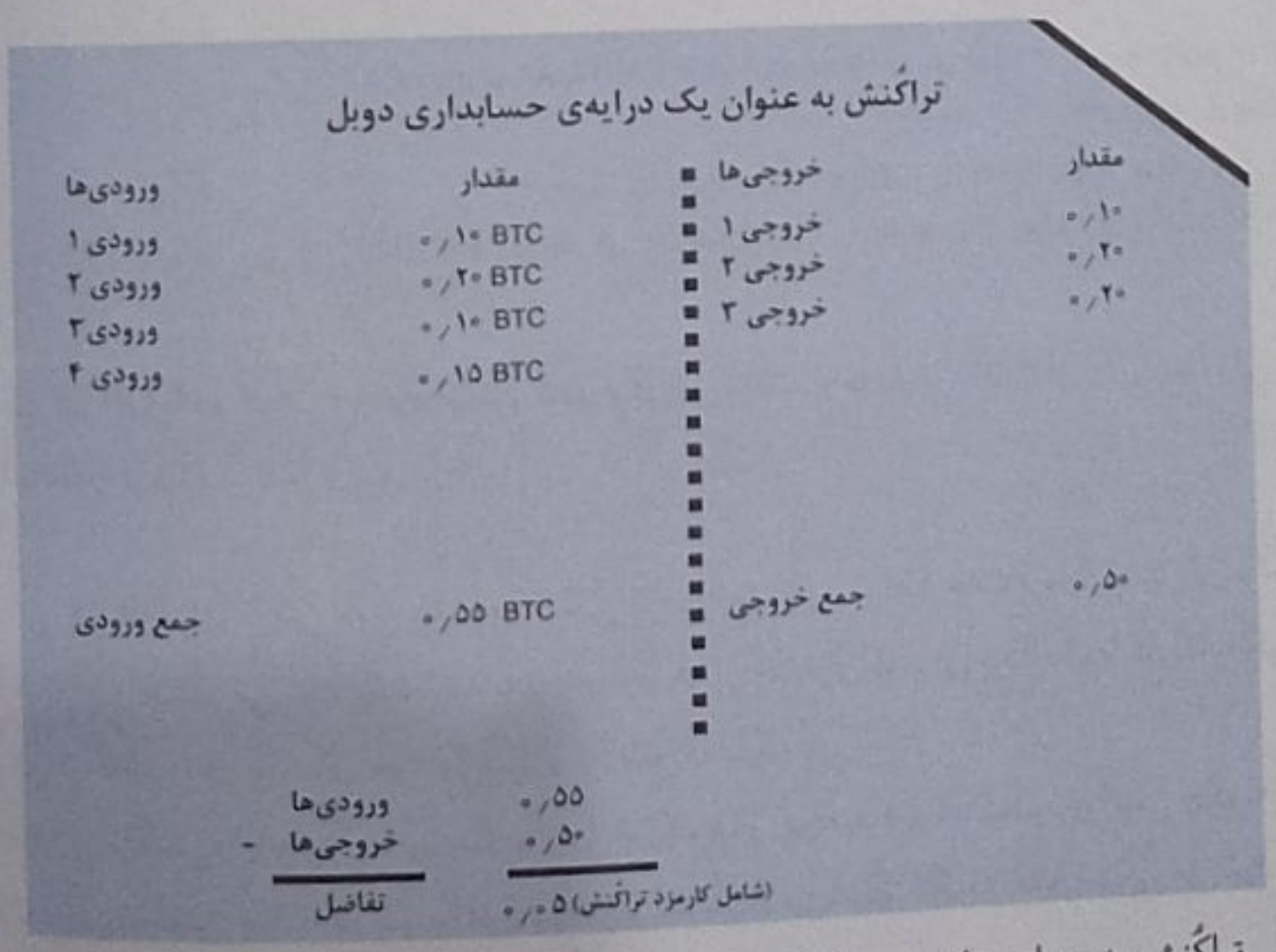
```
https://blockexplorer.com/tx/
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
```

تراکُنش‌های بیت‌کوین

به زبان ساده، یک تراکُنش (transaction) به شبکه می‌گوید که مالک مقداری بیت‌کوین اجازه‌ی انتقال آن به فردی دیگر را صادر کرده است. پس از انجام این تراکُنش، مالک جدید این بیت‌کوین می‌تواند با ایجاد تراکُنش جدید مجوز انتقال آن به دیگران را صادر کند، و این زنجیره‌ی انتقال مالکیت می‌تواند به همین ترتیب و بدون محدودیت تکرار شود.

ورودی و خروجی تراکُنش

تراکُنش‌ها مانند درایه‌های یک دفتر حسابداری دوبل هستند. هر تراکُنش یک یا چند ورودی (input) دارد که معادل *بدهکاری* در یک حساب بیت‌کوین است. در سمت دیگر این تراکُنش یک یا چند خروجی (output) وجود دارد که معادل *بستانکاری* در یک حساب بیت‌کوین هستند. جمع ورودی‌ها و خروجی‌ها (بدهکاری‌ها و بستانکاری‌ها) لزوماً یکسان نیست. به جای آن، مجموع خروجی‌های یک تراکُنش معمولاً قدری کمتر از جمع ورودی‌های آن است که نشانه‌ی وجود کارمزد تراکُنش (transaction fee) است، حق‌الزحمه‌ی نسبتاً ناچیزی که توسط معدنچی ثبت‌کننده‌ی این تراکُنش در دفتر کل (ledger) از آن برداشته (کسر) می‌شود. شکل ۲-۳ یک تراکُنش بیت‌کوین را به عنوان درایه‌ای در یک دفتر کل حسابداری نشان می‌دهد.



شکل ۲-۳ تراکُنش به عنوان درایه‌ی حسابداری دوبل.

در یک تراکُنش بیت‌کوین همچنین به ازای هر مقداری که خرج می‌شود، اثبات مالکیت آن به صورت امضای دیجیتال دارنده (که هر کسی می‌تواند به طور مستقل آن را اعتبارسنجی کند) درج شده است. در واژه‌شناسی بیت‌کوین، «خرج کردن» عبارت است امضای تراکُنشی که یک مقدار را از تراکُنش قبلی به مالک جدیدی که آدرس بیت‌کوین آن مشخص شده، منتقل می‌کند.

زنجیره‌ی تراکُنش

آلیس برای پرداخت پول قهوه‌ی خود در قهوه‌خانه‌ی باب از خروجی یک تراکُنش قبلی (یعنی همان خرید نقدی بیت‌کوین از جو) به عنوان ورودی تراکُنش جدید استفاده می‌کند. این تراکُنش یک مقدار بیت‌کوین را با کلید خصوصی آلیس **قفل** (lock) می‌کند. تراکُنش جدید آلیس در وجه قهوه‌خانه‌ی باب به تراکُنش قبلی به عنوان ورودی ارجاع کرده و یک خروجی جدید برای پرداخت بهای فنجان قهوه و دریافت مابقی آن تولید می‌کند. این تراکُنش‌ها یک **زنجیره** (chain) می‌سازند که در آن ورودی هر تراکُنش متناظر با خروجی تراکُنش قبلی است. کلید خصوصی آلیس امضای لازم برای باز (unlock) کردن آن خروجی قبلی را فراهم می‌آورد، در نتیجه به شبکه‌ی بیت‌کوین ثابت می‌کند که مالک واقعی آن مقدار بیت‌کوین است. آلیس پرداخت بهای قهوه به آدرس باب را به این تراکُنش پیوست می‌کند، در نتیجه باب برای آن که بتواند این بیت‌کوین را خرج کند، «ملزم است» خروجی تراکُنش آلیس را امضا کند. این تراکُنش نشان‌دهنده‌ی انتقال مقدار بیت‌کوین مشخص‌شده بین آلیس و باب است. در شکل ۲-۴ زنجیره‌ی تراکُنش‌ها از جو به آلیس به باب را مشاهده می‌کنید.

آدرس تتمه‌ی پول

در خروجی بسیاری از تراکُنش‌های بیت‌کوین دو آدرس وجود دارد: آدرس مالک جدید و یک آدرس متعلق به مالک فعلی، که به آن آدرس **تتمه** (change address) گفته می‌شود. دلیل آن است که (مانند اسکناس) ورودی یک تراکُنش را نمی‌توان تقسیم کرد. برای مثال، اگر کالایی بخرید که ۱۵۰۰ تومان قیمت داشته باشد و یک اسکناس ۵۰۰۰ تومانی به فروشنده بدهید، طبیعتاً انتظار دارید تتمه‌ی آن، یعنی ۳۵۰۰ تومان، را به شما برگرداند. این مفهوم برای ورودی تراکُنش بیت‌کوین هم مصداق دارد.

شکل ۲-۴ یک زنجیره‌ی تراکُنش، که در آن خروجی یک تراکُنش ورودی تراکُنش بعدی است.

فرض کنید می‌خواهید کالایی بخرید که قیمت آن ۵ بیت‌کوین است ولی فقط یک تراکُنش به ارزش ۲۰ بیت‌کوین دارید؛ در اینجا کیف‌پول شما ۵ بیت‌کوین به فروشنده می‌فرستد و ۱۵ بیت‌کوین تتمه‌ی آن را (بعد از کسر کارمزد تراکُنش) به خودتان برمی‌گرداند. نکته‌ی مهم این است که آدرس تتمه حتماً نباید همان آدرس ورودی باشد، و به خاطر حفظ محرمانگی اغلب برنامه‌های کیف‌پول تتمه‌ی تراکُنش را با یک آدرس جدید ذخیره می‌کنند.

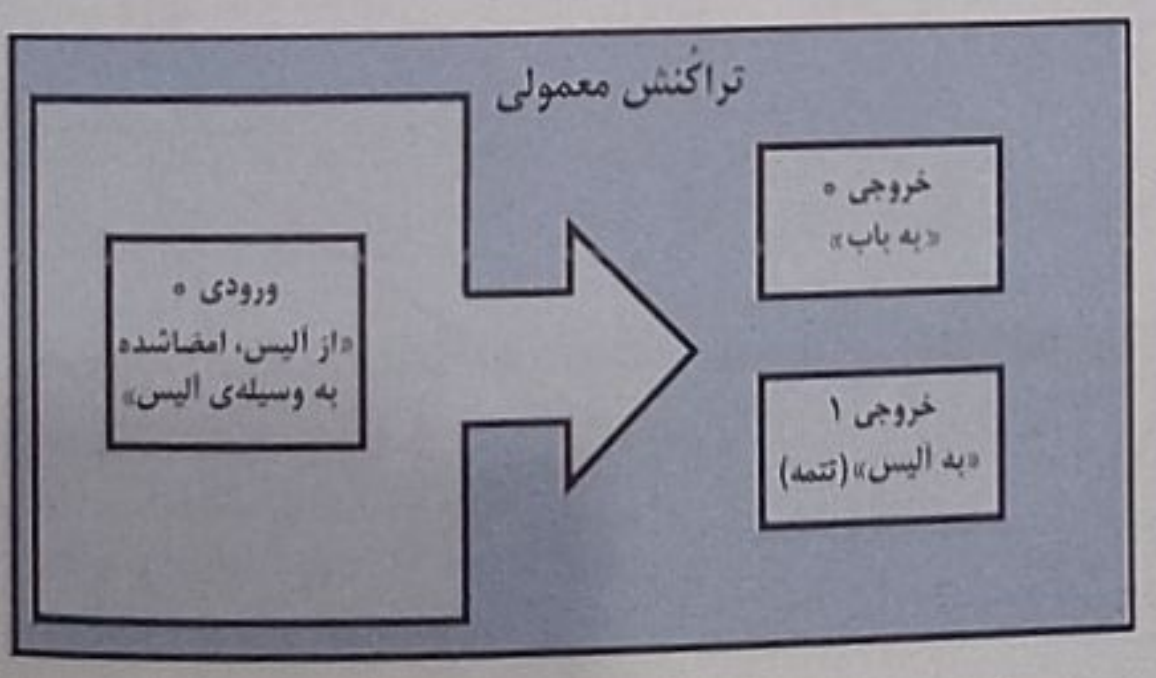
اما اگر در یک کیف‌پول تعداد زیادی تراکُنش با ارزش‌های مختلف وجود داشته باشد، چطور؟ در این قبیل موارد برنامه‌های کیف‌پول مختلف راهبردهای متفاوتی دارند. برخی برنامه‌ها برای انجام یک پرداخت چند ورودی کوچک را با یکدیگر جمع می‌کنند، در حالی که برنامه‌های دیگر ممکن است از یک ورودی واحد که ارزش آن معادل یا بیشتر از مقدار پرداخت مورد نظر باشد، استفاده کنند. اغلب پرداخت‌ها با تتمه همراه است، مگر در موارد نادری که کیف‌پول بتواند چند تراکُنش را طوری با یکدیگر جمع بزند که ارزش آنها درست برابر با پرداخت مورد نظر (به اضافه‌ی کارمزد تراکُنش) شود. رفتار برنامه‌های کیف‌پول درست شبیه خود ما در خرید و فروش با پول نقد است. اگر همیشه پرداخت‌های خود را با درشت‌ترین اسکناسی که در جیب دارید، انجام دهید، سرانجام جیب شما پُر از اسکناس و سکه‌های خُرد خواهد شد. اما اگر تا حد امکان فقط از پول‌های خُرد خود استفاده کنید، همیشه پول درشت خواهید داشت. ما آدم‌ها به طور ناخودآگاه یک نقطه‌ی توازن بین این دو وضعیت انتهایی پیدا می‌کنیم، و برنامه‌نویسان برنامه‌های کیف پول هم دوست دارند راه رسیدن به این نقطه‌ی تعادل را پیدا کنند.

به طور خلاصه، یک *تراکُنش* مقداری بیت‌کوین را از ورودی تراکُنش به خروجی آن منتقل می‌کند. ورودی یک تراکُنش همیشه ارجاعی به خروجی یک تراکُنش قبلی است که نشان می‌دهد این مقدار بیت‌کوین از کجا آمده است. خروجی تراکُنش یک مقدار مشخص بیت‌کوین را به آدرس بیت‌کوین جدید (گیرنده) می‌فرستد و می‌تواند مقداری تتمه نیز داشته باشد که به مالک اولیه برگشت داده خواهد شد. از خروجی یک تراکُنش می‌توان به عنوان ورودی تراکُنش‌های بعدی استفاده کرد، که در نتیجه یک *زنجیره‌ی تراکُنش* بین کاربران شکل می‌گیرد (شکل ۲-۴ را ببینید).

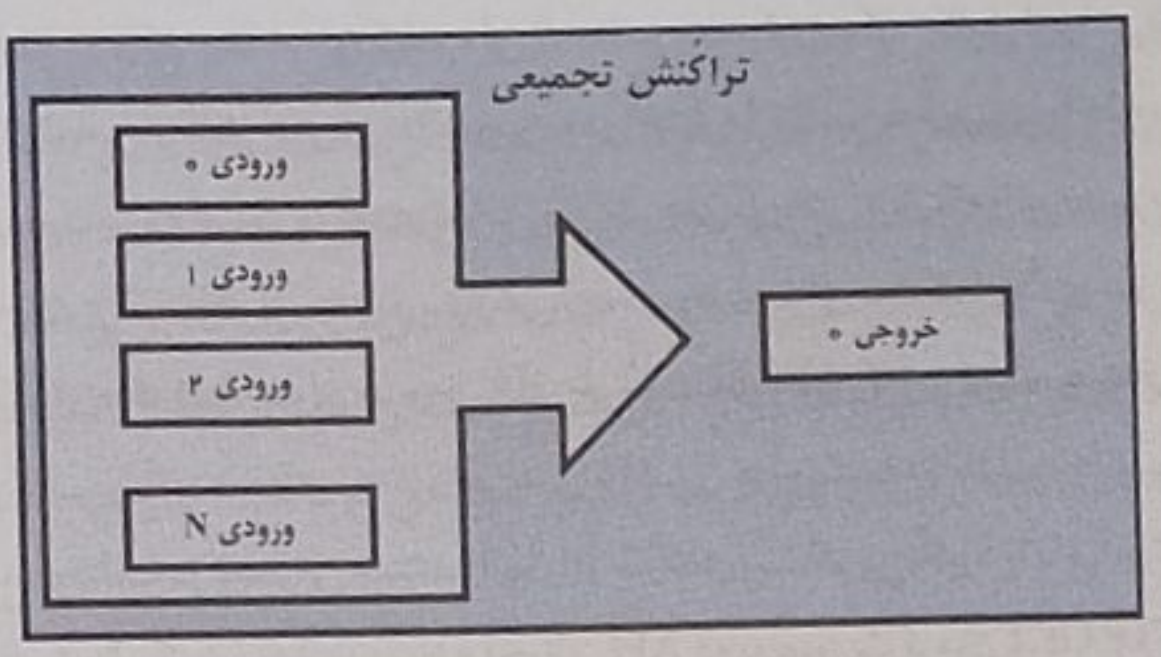
انواع رایج تراکُنش

رایج‌ترین نوع تراکُنش عبارت است از پرداخت ساده از یک آدرس به آدرس دیگر که معمولاً با مقداری «تتمه» (مبلغی که به پرداخت‌کننده برگشت داده می‌شود) همراه است. این نوع تراکُنش یک ورودی و دو خروجی دارد؛ شکل ۲-۵ را ببینید.

نوع دیگری از تراکُنش نیز هست که در آن چندین ورودی با یکدیگر تجمیع شده و یک خروجی واحد می‌سازند (شکل ۲-۶ را ببینید). این تراکُنش معادل حالتی است که برای پرداخت بهای یک کالا تعداد زیادی سکه و اسکناس ریز را به فروشنده می‌دهید. گاهی اوقات برنامه‌های کیف‌پول وقتی تعداد زیادی ورودی ریز دارند (ورودی‌هایی که معمولاً حاصل برگشت تتمه‌ی پول در تراکُنش‌های قبلی هستند)، از این روش برای خلوت کردن کیف‌پول استفاده می‌کنند.



شکل ۲-۵ رایج‌ترین نوع تراکُنش.



شکل ۲-۶ تراکُنشی که چندین ورودی خُرد را تجمیع می‌کند.

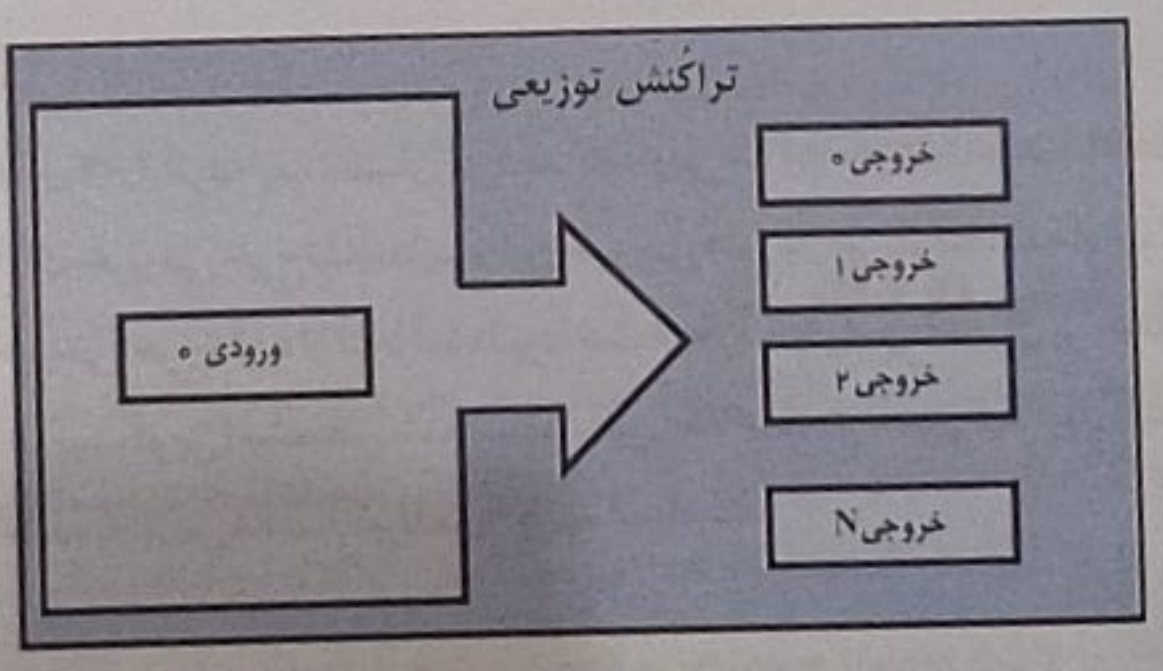
سرانجام، نوع دیگری از تراکُنش که اغلب در دفتر کل بیت‌کوین دیده می‌شود، تراکُنشی است که در آن از یک ورودی برای پرداخت چندین خروجی استفاده شده است (شکل ۲-۷ را ببینید). این نوع تراکُنش برخی اوقات توسط واحدهای تجاری برای توزیع پول (مانند پرداخت حقوق به کارمندان) به کار می‌رود.

ایجاد یک تراکُنش

کیف‌پول آلیس تمام امکانات پردازشی لازم برای انتخاب ورودی و خروجی مناسب برای ایجاد تراکُنش‌های مورد نظر آلیس را در اختیار دارد. فقط کافی است آلیس مقصد (گیرنده) و مقدار پرداخت را به آن بگوید تا این برنامه بقیه‌ی کارها را بدون نیاز به دخالت آلیس انجام دهد. یک برنامه‌ی کیف‌پول قادر است حتی بدون اتصال به اینترنت تراکُنش‌ها را ایجاد کند. درست مثل وقتی که یک چک را در خانه می‌نویسید و امضا می‌کنید و سپس آن را به بانک می‌برید، برای ایجاد و امضا کردن تراکُنش‌ها نیازی به متصل بودن به شبکه‌ی بیت‌کوین نیست.

انتخاب ورودی مناسب

برنامه‌ی کیف‌پول آلیس قبل از هر کاری باید ورودی(های) مناسب برای پرداخت مورد نظر (در اینجا پرداخت پول یک فنجان قهوه به باب) را پیدا کند. اکثر برنامه‌های کیف‌پول فهرست تمامی خروجی موجود متعلق به آدرس‌های آن کیف‌پول را در اختیار دارند. بنابراین، کیف‌پول آلیس حاوی یک نسخه از خروجی تراکُنش دریافت بیت‌کوین از جو است، که (در فصل قبل دیدید)



شکل ۲-۷ تراکُنشی که یک ورودی را بین چندین خروجی توزیع می‌کند.

در ازای پول نقد انجام گرفت. در واقع، برنامه‌های کیف‌پولی که به صورت مشتری گره-کامل اجرا می‌شوند، یک نسخه از تمام خروجی‌های خرج‌نشده از تمامی تراکُنش‌های آن بلاک‌چین را در اختیار دارند. این به کیف‌پول اجازه می‌دهد تا علاوه بر ایجاد ورودی برای تراکُنش‌های خود، بتواند صحت ورودی تمامی تراکُنش‌های دریافتی از شبکه را نیز به سرعت اعتبارسنجی کند. با این حال، از آنجا که یک مشتری گره-کامل به منابع پردازشی (مخصوصاً فضای دیسک) زیادی نیاز دارد، اکثر کیف‌پول‌ها به اجرای یک مشتری «سبک‌وزن» که فقط حاوی خروجی‌های خرج‌نشده‌ی همان کاربر است، بسنده می‌کنند.

اگر یک برنامه‌ی کیف‌پول نسخه‌ای از خروجی‌های تراکُنش خرج‌نشده نداشته باشد، می‌تواند با استفاده از کتابخانه‌هایی که از منابع مختلف در دسترس هستند، آنها را از شبکه‌ی بیت‌کوین بگیرد یا با فراخوانی یک تابع API از یک گره-کامل بپرسد. در مثال ۲-۲ یک نمونه از این نوع فراخوانی API که به صورت فرمان HTTP GET به یک URL خاص ساخته شده، نشان داده شده است. این URL تمام خروجی‌های تراکُنش خرج‌نشده برای آدرس بیت‌کوین مشخص‌شده را برمی‌گرداند، و همه‌ی آنچه برنامه‌ی کیف‌پول برای ایجاد ورودی تراکُنش نیاز دارد، در اختیار آن قرار می‌دهد. ما برای گرفتن پاسخ این سرویس‌دهنده از یک برنامه‌ی مشتری HTTP خط-فرمان ساده به نام *cURL* استفاده کردیم.

مثال ۲-۲ جستجوی تمامی خروجی‌های خرج‌نشده برای آدرس بیت‌کوین آلیس

```
$ 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
    }
  ]
}
```

پاسخی که در مثال ۲-۲ گرفته‌ایم، نشان می‌دهد که آدرس 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (آدرس بیت‌کوین آلیس) یک خروجی خرج‌نشده دارد (و این خروجی هنوز بازپس گرفته نشده است). در این پاسخ همچنین ارجاع تراکُنشی که این خروجی خرج‌نشده از آنجا آمده (پرداخت از طرف جو)، و مقدار آن بر حسب ساتوشی [۱۰ میلیون ساتوشی، معادل یک‌دهم بیت‌کوین] مشخص شده است. با این اطلاعات، برنامه‌ی کیف‌پول آلیس می‌تواند یک تراکُنش برای انتقال مقدار خواسته‌شده به آدرس مالک (گیرنده‌ی) جدید ایجاد کند.

برای دیدن تراکُنش پرداخت از جو به آلیس به https://bit.ly/1tAeeGr نگاه کنید.

همـــان طور که می‌توان دیـــد، در کیف‌پول آلیس آن مقدار بیت‌کوین در یک خروجی خرج‌نشـــده‌ی واحد وجود دارد که برای پرداخت بهای یک فنجان قهوه (صورتحســـاب باب) کافی باشـــد. اگر چنین نباشد، کیف‌پول آلیس مجبور است برای این پرداخت تعداد زیادی خروجی خرج‌نشده‌ی ریز را با یکدیگر تجمیع کند، درست مثل زمانی که سکه‌ها و اسکناس‌های ریز خود را از این جیب و آن جیب جمع می‌کنید تا بتوانید بهای یک کالا را پرداخت کنید. در هر دو حالت، احتمال آن هست که [مانند این مثال] مبلغ خروجی (یا تجمیع چند خروجی) از مقدار لازم برای پرداخت بیشتر باشد و لازم شود تا برنامه‌ی کیف‌پول تتمه‌ی آن را با ایجاد یک تراکُنش خروجی (پرداخت) ثانویه به آلیس برگشت دهد.

ایجاد خروجی

خروجی تراکُنش در واقع یک اســـکریپت است که مقدار مشخص‌شـــده در این خروجی را محبوس می‌کند و فقط با جواب دادن به معمای مطرح‌شده در این اسکریپت می‌توان آن را آزاد (بازیابی) کرد. به زبان ساده‌تر، خروجی تراکُنش آلیس حاوی اســـکریپتی خواهد بود که چنین می‌گوید: «هر کسی که بتواند امضایی متناظر با آدرس عمومی باب ارائه کنـــد، می‌تواند مبلغ موجود در این خروجی را تصاحب کنـــد.» از آنجا که کلید خصوصی متناظر با این آدرس (کلید عمومی) فقط در کیف‌پول باب وجود دارد، فقط کیف‌پول باب است که می‌تواند امضای لازم برای تصاحب این مبلغ را ارائه کند. در حقیقت، آلیس برای آزاد کردن این خروجی امضای باب را طلب می‌کند.

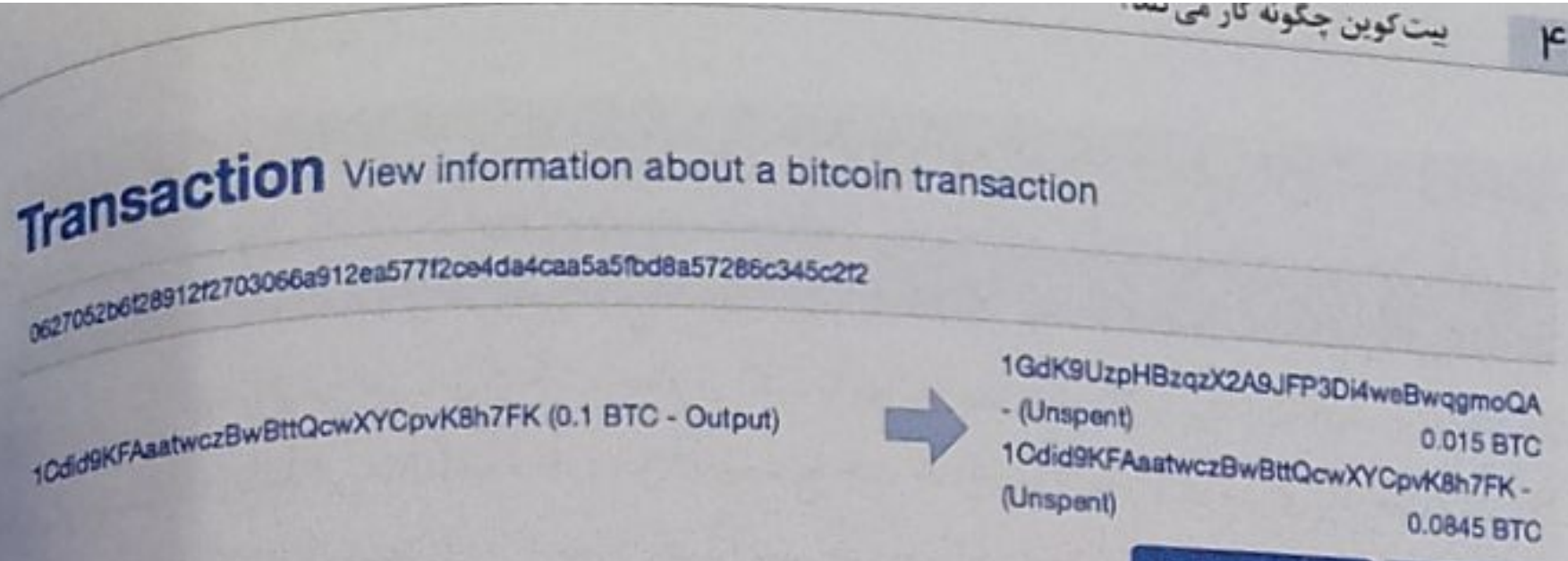
ایـــن تراکُنش حاوی یک خروجی ثانویه نیز هســـت، چون مبلغ ورودی آلیـــس (۰٫۱۰ BTC) از مبلغی که در این تراکُنش باید پرداخت شـــود (۰٫۰۱۵ BTC) بیشتر است. در واقع، مبلغ ۰٫۰۸۵ BTC باید به عنوان تتمه به آلیس برگردانده شود. کیف‌پول آلیس این تتمه را به صورت یک خروجی (درست مثل تراکُنش پرداخت به باب) برمی‌گرداند. در حقیقت، کیف‌پول آلیس مبلغ ورودی تراکُنش را به دو بخش تقســـیم می‌کند: یک بخش را به باب پرداخت می‌کند و بخش دیگر را به خودش. آلیس می‌تواند این خروجی را در تراکُنش‌های بعدی خود خرج کند.

ســـرانجام، برای آن که این تراکُنش به‌موقع و در مدت زمانی مناسب در شبکه پردازش شود، برنامه‌ی کیف‌پول آلیس مبلغی جزئی به‌عنوان *حق‌الزحمه* به آن اضافه خواهد کرد. این حق‌الزحمه به طور صریح در تراکُنش ظاهر نمی‌شود، بلکه خود را به صورت اختلاف بین ورودی و خروجی(ها) نشان می‌دهد. اگر کیف‌پول آلیس به جای تتمه‌ای به مقدار ۰٫۰۸۵ BTC، خروجی دوم را فقط به مبلغ ۰٫۰۸۴۵ BTC ایجاد کند، مقدار ۰٫۰۰۰۵ BTC (نیم میلی‌بیت‌کوین) باقی خواهد ماند. اگر دو خروجی این تراکُنش را جمع بزنیم، مجموع آنها از ۰٫۱۰ BTC (ورودی تراکُنش) کمتر خواهد شد. این اختلاف همان *کارمزد تراکُنش* است که معدنچی به عنوان حق‌الزحمه‌ی اعتبارسنجی تراکُنش و اضافه کردن آن به یک بلاک برای ثبت در بلاک‌چین برای خود برمی‌دارد. این تراکُنش را می‌توان به کمک یک برنامه‌ی کاوشگر بلاک‌چین مشاهده کرد (شکل ۲-۸ را ببینید).

برای دیدن تراکُنش پرداخت از آلیس به قهوه‌خانه‌ی باب به https://bit.ly/1u0FIGs نگاه کنید.

اضافه کردن تراکُنش به دفتر کل

تراکُنش ایجادشـــده توسط کیف‌پول آلیس ۲۵۸ بایت است و هر چیزی را که برای اثبات مالکیت این مبلغ و تصاحب آن توســـط مالک جدید لازم باشـــد، در خود دارد. اکنون این تراکُنش باید به شبکه‌ی بیت‌کوین ارسال شود تا بتواند به بخشـــی از بلاک‌چین تبدیل شود. در قسمت بعد خواهیم دید که این تراکُنش چگونه بخشی از یک بلاک جدید شده، و این بلاک چگونه «اســـتخراج می‌شود». سرانجام خواهیم دید چگونه اعتماد به این بلاک جدید (بعد از اضافه شدن به بلاک‌چین) با اضافه شدن بلاک‌های بعدی به طور روزافزون افزایش می‌یابد.



شکل ۲-۸ تراکُنش پرداخت آلیس به قهوه‌خانه‌ی باب.

ارسال تراکُنش

از آنجـا که این تراکُنش حاوی تمام اطلاعات لازم برای پردازش اسـت، فرقی نمی‌کند چگونه و در چه زمانی به شـبکه‌ی بیت‌کوین ارسال شود. شبکه‌ی بیت‌کوین یک *شبکه‌ی همتا-به-همتا* است، که در آن هر گره (مشتری بیت‌کوین) به چندین گره دیگر متصل است. هدف اصلی این شبکه منتشر کردن تراکُنش‌ها و بلاک‌ها بین تمامی اعضای آن است.

چگونگی انتشار تراکُنش

هر سیسـتمی (سرویس‌دهنده‌ی وب، برنامه‌ی کاربردی، یا کیف‌پول موبایل) که با «حرف زدن» به زبان پروتکل بیت‌کوین در شبکه‌ی بیت‌کوین مشارکت داشته باشـد، یک **گره بیت‌کوین** (bitcoin node) نامیده می‌شود. برنامه‌ی کیف‌پول آلیس می‌تواند این تراکُنش جدید را از هر طریقی که بخواهد (شبکه‌ی کابلی، وای-فای، تلفن همراه)، به گره‌هایی بیت‌کوینی که به آنها متصل است، بفرستد. نیازی نیست کیف‌پول بیت‌کوین آلیس به طور مستقیم به کیف‌پول بیت‌کوین باب متصل باشد، و همچنین آلیس مجبور نیسـت از همان اتصال اینترنت قهوه‌خانه‌ی باب استفاده کند (هر چند این گزینه‌ها هر دو محتمل هستند). هر گره بیت‌کوین که یک تراکُنش معتبر دریافت کند که قبلاً آن را ندیده باشد، بلافاصله آن را به تمام گره‌هایی که به آنها متصل است، می‌فرستد؛ این روش انتشار به **سیل آسا** (flooding) معروف است. در نتیجه‌ی این تکنیک، تراکُنش آلیس به سرعت روی شبکه‌ی همتا-به-همتا منتشر می‌شود، و در عرض چند ثانیه به درصد بالایی از گره‌های شبکه می‌رسد.

روند وقایع از دید باب

اگر برنامه‌ی کیف‌پول بیت‌کوین باب به طور مسـتقیم به برنامه‌ی کیف‌پول آلیس متصل باشد، کیف‌پول باب یکی از اولین گره‌هایی خواهد بود که این تراکُنش را دریافت می‌کنند. با این حال، حتی اگر کیف‌پول آلیس این تراکُنش را از طریق گره‌های دیگر ارسـال کند، کیف‌پول باب چند ثانیه بعد آن را دریافت خواهد کرد. کیف‌پول باب بلافاصله تراکُنش آلیس را به عنوان یک *پرداخت ورودی* تشـخیص می‌دهد، چون کلید لازم برای باز کردن و تصاحب مبلغ درون آن را در اختیار دارد. برنامه‌ی کیف‌پول باب همچنین می‌تواند به طور مستقل سلامت ساختار این تراکُنش، استفاده از ورودی‌های قبلاً خرج‌نشده در آن، و

وجود کارمزد کافی برای اضافه شدن به بلاک بعدی را تشخیص دهد. در این نقطه باب می‌تواند (با کمی خطر) فرض را بر آن بگذارد که این تراکُنش به زودی در یک بلاک قرار گرفته و تأیید خواهد شد.

توجه

یکی از تصورات نادرست رایج درباره‌ی تراکُنش‌های بیت‌کوین این است که آنها باید بعد از ۱۰ دقیقه انتظار برای یک بلاک جدید، یا حداکثر ۶۰ دقیقه برای شش تأییدیه کامل، تأیید شوند. هر چند تأییدیه‌ها به معنای آن هستند که یک تراکُنش در کل شبکه پذیرفته شده است، چنین تأخیری برای تراکُنش‌های با مبلغ اندک (مثل خرید یک فنجان قهوه) غیرضروری است. خطر پذیرفتن تراکُنش‌های کم-مبلغ بدون داشتن تأییدیه بیشتر از پذیرش کارت‌های اعتباری بدون مطالبه‌ی کارت شناسایی یا امضای صورتحساب (که امروزه به رویه‌ای رایج در بازار تبدیل شده) نیست.

استخراج بیت‌کوین

تراکُنش آلیس اکنون روی شبکه‌ی بیت‌کوین منتشر شده است، اما تا زمانی که طی فرآیندی موسوم به **استخراج** (mining) اعتبارسنجی نشود و در یک بلاک قرار نگیرد، به بخشی از بلاک‌چین تبدیل نخواهد شد. (برای اطلاعات بیشتر درباره‌ی استخراج بیت‌کوین به فصل ۱۰ نگاه کنید.)

گفتیم که سیستم بیت‌کوین بر اعتماد استوار است و این اعتماد بر اساس محاسبه (پردازش) شکل می‌گیرد. تراکُنش‌ها به صورت بلاک بسته‌بندی (تجمیع) می‌شوند، فرآیندی که اثبات آن به مقدار بسیار زیادی محاسبات نیاز دارد، ولی همین که یک تراکُنش اثبات شد، بررسی صحت و سقم آن فقط مقدار کمی محاسبه نیاز خواهد داشت. فرآیند استخراج در بیت‌کوین دو هدف را دنبال می‌کند:

- گره‌های استخراج‌کننده با ارجاع به **قواعد اجماع** (consensus rules) بیت‌کوین تمام تراکُنش‌ها را اعتبارسنجی می‌کنند. بنابراین، فرآیند استخراج با رد تراکُنش‌های ناقص یا دارای ساختار نامناسب، امنیت تراکُنش‌های بیت‌کوین را تضمین می‌کند.
- فرآیند استخراج باعث خلق بیت‌کوین‌های جدید در هر بلاک می‌شود، درست مثل بانک‌های مرکزی که پول جدید چاپ می‌کنند. مقدار تولید بیت‌کوین در هر بلاک محدود است و به مرور زمان، بر اساس یک جدول ثابت زمان‌بندی نشر، کاهش می‌یابد.

در استخراج بیت‌کوین یک توازن ظریف بین هزینه و جایزه (reward) برقرار شده است. فرآیند استخراج مستلزم صرف انرژی (برق) برای حل یک مسأله‌ی ریاضی است. یک معدنچی موفق *جایزه* (پاداش) خود را به صورت سکه‌های بیت‌کوین جدید و کارمزد تراکُنش دریافت می‌کند. با این حال، این معدنچی فقط زمانی می‌تواند پاداش خود را تصاحب کند که تمامی تراکُنش‌ها را به درستی، و با رعایت قواعد اجماع، اعتبارسنجی کرده باشد. همین توازن ظریف است که امنیت بیت‌کوین را بدون وجود یک مرجع رسمی مرکزی تأمین می‌کند.

فرآیند استخراج را می‌توان مثل یک بازی فکری (مانند سودوکو) غول‌آسا تصور کرد که عده‌ی زیادی همزمان برای حل آن تلاش می‌کنند و هر بار که کسی آن را حل می‌کند، بازی از اول شروع می‌شود. سختی این بازی به طور خودکار طوری تنظیم می‌شود که تقریباً هر ۱۰ دقیقه یک بار بتوان آن را حل کرد. یک سودوکوی غول‌آسا با هزاران سطر و ستون را در نظر بگیرید؛ اگر یک سودوکوی حل‌شده را به شما نشان دهند، به سرعت می‌توانید درستی آن را بررسی کنید. با این حال، اگر فقط تعداد کمی از خانه‌ها پُر شده باشند، حل کردن آن به تلاش فکری بسیار زیادی نیاز دارد! دشواری سودوکو را می‌توان با تغییر دادن اندازه‌ی بازی (تعداد سطرها و ستون‌ها) تنظیم کرد، ولی وقتی یک سودوکو حل شده باشد، تشخیص درستی حل آن (هر

قدر هم که بزرگ باشد) به سادگی میسر است. «معما»یی که کاربران بیت‌کوین باید حل کنند، نوعی دَرهم‌سازی رمزنگاری است که خصوصیات مشابهی دارد: این معما به شدت نامتقارن است، یعنی حل کردن آن بسیار دشوار، ولی تشخیص درستی معمای حل‌شده ساده است؛ و دشواری آن را نیز می‌توان تنظیم (کم یا زیاد) کرد.

یکی دیگر از افرادی که در فصل قبل با او آشنا شدیم، جینگ (دانشجوی کارآفرین اهل شانگهای) است. جینگ یک **مزرعه‌ی استخراج** (mining farm) راه انداخته است، هزاران کامپیوتر تخصصی استخراج بیت‌کوین که برای به دست آوردن پاداش با دیگر کاربران شبکه رقابت می‌کنند. در هر ۱۰ دقیقه (یا همین حدود)، کامپیوترهای معدنکاوی جینگ وارد یک رقابت شدید با هزاران سیستم مشابه در سرتاسر دنیا می‌شوند تا معمای یک بلاک از تراکُنش‌ها را حل کنند. پیدا کردن جواب این معما، که به آن اثبات-کار (Proof-of-Work) یا به اختصار **PoW** گفته می‌شود، مستلزم هزاران تریلیون عمل دَرهم‌سازی در هر ثانیه (در سرتاسر شبکه‌ی بیت‌کوین) است. الگوریتم اثبات-کار عبارت است از دَرهم‌سازی مکرر سرآیند بلاک مورد نظر به اضافه‌ی یک رشته‌ی تصادفی با الگوریتم رمزنگاری SHA256، تا زمانی که یک جواب با الگویی از پیش‌تعیین‌شده به دست آید. اولین معدنچی که به این جواب برسد، آن دور از مسابقه را می‌برد و آن بلاک را در بلاک‌چین ثبت می‌کند.

جینگ استخراج بیت‌کوین و یافتن PoW بلاک‌های جدید را از سال ۲۰۱۰ با استفاده از یک کامپیوتر رومیزی بسیار پُرسرعت شروع کرد. با ورود معدنچیان جدید به شبکه‌ی بیت‌کوین، دشواری معمای بیت‌کوین به سرعت بالا رفت. بعد از مدتی، جینگ و سایر معدنچیان به سخت‌افزارهای تخصصی پیشرفته برای استخراج بیت‌کوین روی آوردند، مانند پردازنده‌های گرافیکی (GPU) اختصاصی قدرتمند که در کامپیوترها و کنسول‌های بازی به کار می‌روند. امروزه معمای بیت‌کوین چنان سخت شده که استخراج آن فقط با استفاده از پردازنده‌های بسیار خاص موسوم به ASIC مقرون به صرفه است؛ در یک پردازنده‌ی ASIC صدها یا هزاران مدار مجتمع مینیاتوری که به طور اختصاصی برای حل معمای رمزنگاری بیت‌کوین طراحی شده‌اند، روی یک تراشه‌ی سیلیکونی واحد کاشته شده‌اند و به طور موازی کار می‌کنند. شرکت جینگ به **استخراج گروهی** (pool mining) یا *استخراج ائتلافی* نیز روی آورده است؛ در این رویکرد چندین مشتری در استخراج یک بلاک همکاری کرده و سپس جایزه‌ی آن را به نسبت سهم هر یک از آنها در تولید این بلاک تقسیم می‌کنند. مزرعه‌ی شرکت جینگ امروزه مشتمل بر هزاران دستگاه معدنچی ASIC است که به طور شبانه‌روزی مشغول استخراج بیت‌کوین هستند. این کامپیوترها مقدار بسیار زیادی برق مصرف می‌کنند که هزینه‌ی آن (و سایر هزینه‌های شرکت) از فروش بیت‌کوین‌های استخراج‌شده به دست می‌آید، و البته مقداری سود هم برای جینگ باقی می‌مانند.

استخراج تراکُنش‌های یک بلاک

کیف‌پول کاربران و سایر برنامه‌ها به طور پیوسته تراکُنش‌های جدید ایجاد کرده و وارد شبکه‌ی بیت‌کوین می‌کنند. وقتی این تراکُنش‌ها به گره‌های شبکه‌ی بیت‌کوین می‌رسند، به مخزن موقت تراکُنش‌های تأییدنشده که در هر گره نگهداری می‌شوند، می‌روند. همان طور که معدنچیان یک بلاک جدید می‌سازند، تراکُنش‌های تأییدنشده را از این مخزن به بلاک جدید اضافه کرده، و سپس تلاش می‌کنند با الگوریتم استخراج (الگوریتم اثبات-کار) اعتبار این بلاک جدید را اثبات کنند. جزئیات این فرآیند را به طور مفصل در فصل ۱۰ توضیح خواهیم داد.

تراکُنش‌ها به این بلاک جدید اضافه شده، و بر اساس مبلغ تراکُنش (از زیاد به کم) و چند معیار دیگر اولویت‌بندی می‌شوند. هر معدنچی فرآیند استخراج یک بلاک جدید از تراکُنش‌های واردشده را به محض دریافت پاسخ بلاک قبلی از شبکه شروع می‌کند، چون می‌داند که دیگر شانسی برای برنده شدن در مسابقه‌ی دور قبل ندارد. او بلافاصله یک بلاک جدید ایجاد می‌کند، و سپس آن را با تراکُنش‌ها و اثر انگشت بلاک قبلی پُر کرده و شروع به محاسبه‌ی PoW برای این بلاک جدید می‌کند. هر معدنچی یک تراکُنش ویژه در بلاک خود قرار می‌دهد، تراکُنشی که جایزه‌ی آن بلاک (که مقدار آن در حال حاضر ۱۲٫۵ بیت‌کوین جدید است) به اضافه مجموع کارمزد تمامی تراکُنش‌های موجود در این بلاک را به آدرس بیت‌کوین او پرداخت می‌کند. اگر او موفق به یافتن جوابی شود که باعث معتبر شدن این بلاک می‌شود، برنده‌ی این جایزه خواهد شد، چون

این بلاک است که به بلاک‌چین جهانی اضافه شده و تراکُنش جایزه‌ی او را قابل خرج کردن می‌کند. جینگ که در یک مزرعه‌ی استخراج گروهی فعالیت دارد، نرم‌افزار خود را طوری پیکربندی کرده که جایزه‌ی بلاک‌های جدید را به آدرس بیت‌کوین گروه می‌فرستد. در آنجا است که این جایزه بر حسب سهم هر معدنچی (در آخرین دور مسابقه) تقسیم شده و به آدرس بیت‌کوین او پرداخت می‌شود.

شبکه‌ی بیت‌کوین بعد از دریافت تراکُنش آلیس آن را در مخزن تراکُنش‌های تأییدنشده قرار داد. همین که این تراکُنش توسط نرم‌افزار استخراج اعتبارسنجی شد، در یک بلاک جدید، موسوم به **بلاک نامزد** (candidate block) که توسط گروه استخراج جینگ ایجاد شده بود، قرار گرفت. تمام معدنچیان عضو این گروه بلافاصله شروع به محاسبه‌ی PoW این بلاک نامزد کردند. تقریباً پنج دقیقه بعد از آن که کیف‌پول آلیس این تراکُنش را ارسال کرد، یکی از معدنچیان ASIC گروه جینگ جواب معمای این بلاک را پیدا کرده و آن را به شبکه‌ی بیت‌کوین اعلام کرد. همین که معدنچیان دیگر اعتبار این بلاک برنده را تأیید کردند، مسابقه‌ی قبلی را رها کرده و یک مسابقه جدید (برای ایجاد بلاک بعدی) را شروع کردند.

بلاک برنده‌ی جینگ با شماره‌ی ۲۷۷۳۱۶، شامل ۴۲۰ تراکُنش، از جمله تراکُنش آلیس، به بخشی از بلاک‌چین تبدیل شد. این بلاک [برنده] که شامل تراکُنش آلیس است، به عنوان یک «تأییدیه» برای تراکُنش او شمرده می‌شود.

توجه

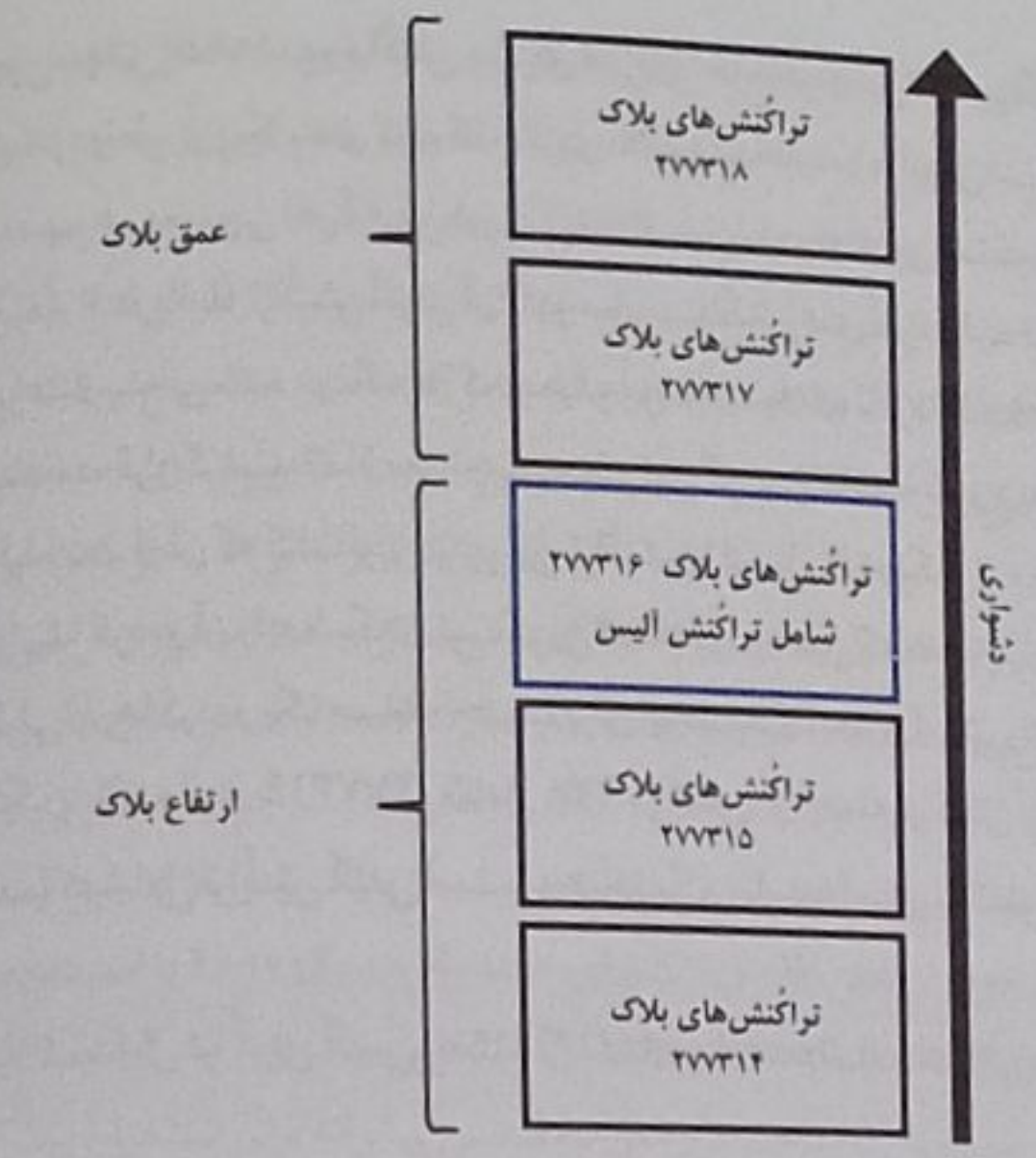
برای دیدن بلاک شامل تراکُنش آلیس به https://blockchain.info/block-height/277316 نگاه کنید.

حدود ۱۰ دقیقه بعد، یک معدنچی دیگر بلاک جدیدی با شماره‌ی ۲۷۷۳۱۷ استخراج می‌کند. از آنجا که این بلاک جدید روی بلاک ۲۷۷۳۱۶ (که شامل تراکُنش آلیس است) ساخته شده، محاسبات بیشتری به بلاک‌چین اضافه کرده و میزان اعتماد به این تراکُنش‌ها را تقویت می‌کند. هر بلاک استخراج‌شده‌ی جدید که روی بلاک مشتمل بر تراکُنش آلیس ساخته شود، یک تأییدیه‌ی اضافی برای این تراکُنش به حساب می‌آید. با انباشته شدن بلاک‌ها روی یکدیگر، احتمال نقض (فسخ) آنها به طور نمایی کمتر و کمتر شده، و در نتیجه میزان اعتماد شبکه به آن بیشتر و بیشتر خواهد شد.

در نمودار شکل ۲-۹ می‌توانیم بلاک ۲۷۷۳۱۶ را که شامل تراکُنش آلیس است، مشاهده کنیم. زیر این بلاک ۲۷۷۳۱۶ بلاک (از جمله ۰) قرار گرفته‌اند که زنجیروار تا اولین بلاک [بلاک ۰، که به آن **بلاک زاینده** (genesis block) یا *بلاک سرآغاز* نیز گفته می‌شود] به یکدیگر وصل شده‌اند؛ نام بلاک‌چین (زنجیره‌ی بلاک) از همین جا آمده است. به مرور زمان، با افزایش «ارتفاع» بلاک‌ها، دشواری محاسبه برای بلاک‌های جدید [و بلاک‌چین، به عنوان یک کل] افزایش می‌یابد. بلاک‌هایی که بعد از بلاک ۲۷۷۳۱۶ (بلاک شامل تراکُنش آلیس) استخراج شده‌اند، اعتماد به این تراکُنش را بالاتر می‌برند، چون هر چه یک زنجیره بزرگتر شود، مقدار محاسبات صرف‌شده (کار انجام‌شده) برای ساخت آن نیز بیشتر خواهد شد. بنا بر قرارداد، بلاک‌هایی که بیش از شش تأییدیه داشته باشند، *برگشت‌ناپذیر* (غیرقابل‌فسخ) تلقی می‌شوند، چون میزان محاسبات مورد نیاز برای فسخ (نامعتبر کردن) این شش بلاک و محاسبه‌ی مجدد آنها فوق‌العاده زیاد خواهد بود. [برای جزئیات بیشتر درباره‌ی فرآیند استخراج و چگونگی تولید اعتماد در شبکه‌ی بیت‌کوین به فصل ۱۰ نگاه کنید.]

خرج کردن تراکُنش

اکنون که تراکُنش آلیس به عنوان بخشی از یک بلاک در بلاک‌چین قرار گرفته، به بخشی از دفتر کل بیت‌کوین تبدیل شده است و تمام برنامه‌های بیت‌کوین می‌توانند آن را ببینند. هر مشتری بیت‌کوین می‌تواند به طور مستقل اعتبار و قابل خرج بودن این تراکُنش را بررسی کند. مشتری‌های گره-کامل می‌توانند سرچشمه‌ی این مبلغ را از لحظه‌ای که این بیت‌کوین برای اولین بار در یک بلاک تولید شده، ردیابی کنند و تراکُنش به تراکُنش جلو بروند تا به آدرس باب برسند. مشتری‌های سبک‌وزن می‌توانند با تأیید این که این تراکُنش جزئی از بلاک‌چین است و بعد از آن چندین بلاک دیگر استخراج شده، و اطمینان از این که تمام معدنچی‌ها آن را به عنوان یک تراکُنش معتبر پذیرفته‌اند، کاری را انجام دهند که به آن **اعتبارسنجی پرداخت ساده** (SPV) گفته می‌شود. [برای اطلاعات بیشتر درباره‌ی SPV به فصل ۸ نگاه کنید.]

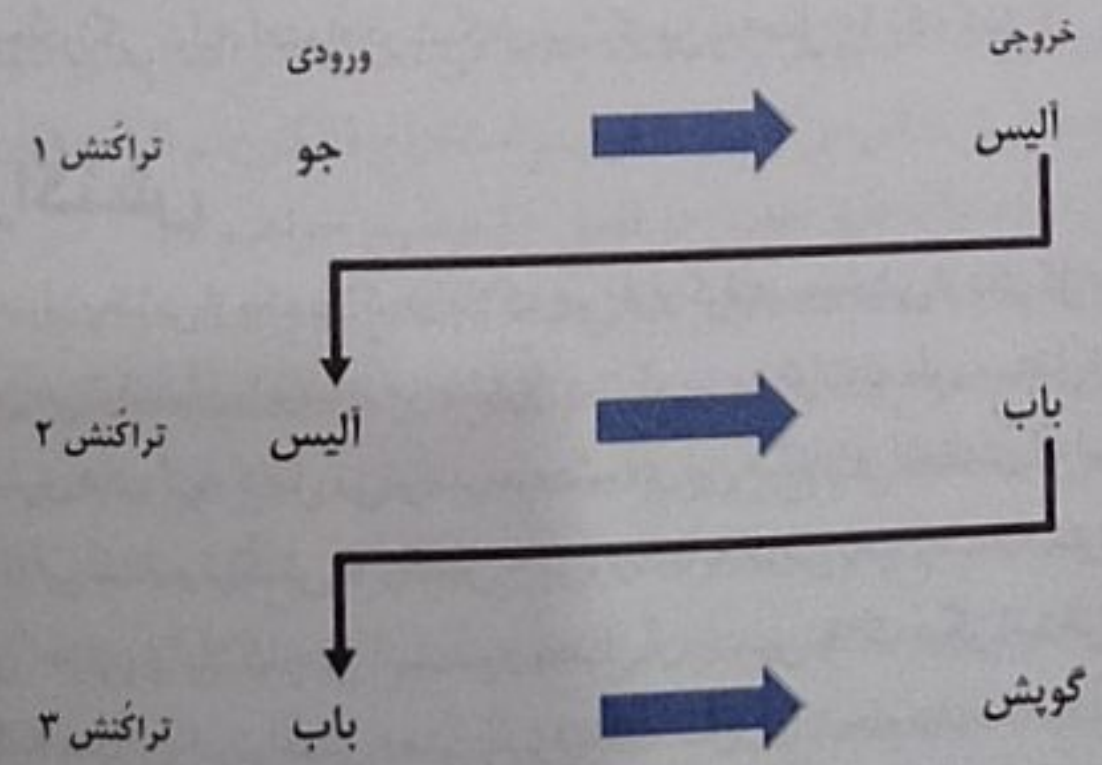


شکل ۲-۹ قرار گرفتن تراکُنش آلیس در بلاک ۲۷۷۳۱۶.

باب اکنون می‌تواند خروجی این تراکُنش و تراکُنش‌های دیگر را خرج کند، مثلاً با آن بخشی از هزینه‌های مغازه‌ی خود را بپردازد. اما به احتمال قویتر، نرم‌افزار بیت‌کوین باب این تراکُنش را با تعدادی تراکُنش ریز دیگر تجمیع می‌کند تا بتواند یک پرداخت درشت انجام دهد. با تجمیع تراکُنش‌های ریز، باب می‌تواند یک خروجی واحد (و یک آدرس بیت‌کوین واحد) با مبلغ قابل توجه داشته باشد. برای دیدن طرز کار یک تراکُنش تجمیعی به شکل ۲-۶ نگاه کنید.

همان طور که باب مبلغ پرداختی آلیس و دیگر مشتریان خود را دریافت و خرج می‌کند، *زنجیره‌ی تراکُنش* را گسترش می‌دهد. برای مثال، فرض کنید باب دستمزد گوپش (طراح سایت وب اهل بنگلور، هندوستان) را با بیت‌کوین پرداخت می‌کند؛ در این حالت، این زنجیره‌ی تراکُنش به صورتی که در شکل ۲-۱۰ می‌بینید، در خواهد آمد.

در این فصل دیدیم تراکُنش‌ها چگونه زنجیره‌ای می‌سازند که مبالغ بیت‌کوین را از یک نفر به نفر دیگر منتقل می‌کند. همچنین، تراکُنش آلیس را از لحظه‌ی ایجاد آن در کیف‌پول او، و مسیری که در شبکه‌ی بیت‌کوین طی کرد تا سرانجام توسط یک معدنچی در بلاک‌چین ثبت شد، دنبال کردیم. در ادامه‌ی کتاب به بررسی فناوری‌های خاصی می‌پردازیم که در پشت صحنه‌ی برنامه‌های کیف‌پول، آدرس‌های بیت‌کوین، امضا، تراکُنش، شبکه‌ی بیت‌کوین، و بالاخره استخراج بیت‌کوین مشغول فعالیت هستند.



شکل ۲-۱۰ تراکُنش آلیس به عنوان بخشی از زنجیره‌ی تراکُنش از جو تا گوپش.