فصل

۱

مقدمه

بیت‌کوین چیست؟

بیت‌کوین مجموعه‌ای از مفاهیم و فناوری‌ها است که مبنای یک زیست‌بوم پول دیجیتال را شکل می‌دهند. پولی که بیت‌کوین نام گرفته، در شبکه‌ی *بیت‌کوین* بین دارندگان آن مبادله می‌شود. کاربران بیت‌کوین برای مبادله‌ی آن از *پروتکل بیت‌کوین* و زیرساخت‌های اینترنت استفاده می‌کنند، هر چند راه‌های دیگری نیز برای مبادله‌ی آن وجود دارد. پشته‌ی پروتکل بیت‌کوین، که به صورت یک نرم‌افزار منبع-باز در دسترس همگان قرار دارد، روی طیف وسیعی از دستگاه‌های کامپیوتری، از کامپیوترهای رومیزی و قابل‌حمل گرفته تا تلفن‌های هوشمند، اجرا می‌شود و دسترسی به این فناوری را بسیار آسان کرده است.

تقریباً هر کاری که با پول‌های سنتی قابل انجام است، خرید و فروش کالا و خدمات، حواله‌ی پول به افراد و شرکت‌ها، و تأمین اعتبار پروژه‌ها، با بیت‌کوین نیز می‌توان انجام داد. بیت‌کوین را می‌توان خرید، فروخت، یا (با نرخ‌های مشخص) به ارزهای دیگر تبدیل (تسعیر) کرد. از یک دیدگاه، بیت‌کوین پولی ایده‌آل برای اینترنت محسوب می‌شود چون سریع، امن و بدون‌مرز است.

اما بر خلاف پول‌های سنتی، بیت‌کوین کاملاً مجازی است. بیت‌کوین هیچ گونه اسکناس یا سکه‌ی فیزیکی ندارد، حتی از نوع دیجیتال آن. سکه‌های بیت‌کوین در واقع چیزی نیستند جز اعداد و رقم‌هایی که در تراکُنش‌ها بین فرستنده و گیرنده مبادله می‌شوند. دارندگان بیت‌کوین فقط صاحب کلیدهایی هستند که اجازه می‌دهند در شبکه‌ی بیت‌کوین مالکیت خود بر [سکه‌های] بیت‌کوین در حال مبادله را اثبات کنند. با این کلیدها می‌توانید تراکُنش‌ها را امضا کرده و قفل آنها را باز کنید؛ پس از آن می‌توانید این پول را (با ارسال به دیگران) خرج کنید. این کلیدها معمولاً در یک کیف‌پول دیجیتال (در کامپیوتر یا تلفن هوشمند کاربر) نگهداری می‌شوند. داشتن کلیدی که بتوان با آن تراکُنش‌ها را امضا کرد، تنها پیش‌نیاز خرج کردن بیت‌کوین است، و اجازه‌ی کنترل کامل آن را به کاربر می‌دهد.

بیت‌کوین یک سیستم همتا-به-همتا (peer-to-peer) توزیع‌شده (distributed) است. به بیان دیگر، بیت‌کوین هیچ سرویس‌دهنده یا نقطه‌ی کنترل «مرکزی» ندارد. بیت‌کوین از طریق فرآیندی موسوم به استخراج (mining) تولید می‌شود، که متضمن رقابت برای یافتن جواب یک مسأله‌ی ریاضی (در کنار پردازش تراکُنش‌ها) است. هر عضو شبکه‌ی بیت‌کوین،

یعنی هر کسی که در حال اجرای پشته‌ی پروتکل بیت‌کوین (bitcoin protocol stack) کامل روی کامپیوتر یا تلفن هوشمند خود باشد، می‌تواند با استفاده از توان پردازشی کامپیوتر خود برای اعتبارسنجی و ثبت تراکُنش‌ها، به عنوان یک معدنچی (miner) شروع به استخراج بیت‌کوین کند. به طور میانگین، یک معدنچی بیت‌کوین می‌تواند در هر ۱۰ دقیقه تراکُنش‌های ۱۰ دقیقه‌ی گذشته را اعتبارسنجی کرده و یک بیت‌کوین جدید جایزه بگیرد. از لحاظ نظری، فرآیند استخراج بیت‌کوین می‌تواند کارکردهای اصلی یک بانک مرکزی، یعنی انتشار پول و تسویه‌حساب بین‌بانکی، را به صورت غیرمتمرکز در آورده و جایگزین این بخش از وظایف بانک‌های مرکزی شود.

پروتکل بیت‌کوین شامل تعدادی الگوریتم داخلی است که فعالیت‌های استخراج بیت‌کوین در سرتاسر شبکه را تنظیم می‌کنند. دشواری وظایف پردازشی که معدنچیان باید انجام دهند، همیشه به طور پویا به گونه‌ای تنظیم می‌شود که صرفنظر از تعداد معدنچیانی که در هر لحظه در حال رقابت هستند (و مقدار توان پردازشی که مصرف می‌شود)، هر فرد به طور میانگین در هر ۱۰ دقیقه موفق به اعتبارسنجی یک بلاک از تراکُنش‌ها شود. این پروتکل همچنین در هر ۴ سال آهنگ تولید بیت‌کوین‌های جدید را نصف می‌کند، به طوری که تعداد کل بیت‌کوین‌هایی که برای همیشه تولید خواهند شد، هرگز از ۲۱ میلیون سکه فراتر نخواهد رفت. در نتیجه تعداد بیت‌کوین‌های در گردش تقریباً همیشه به آسانی قابل تخمین بوده و پیش‌بینی می‌شود که تا سال ۲۱۴۰ به سقف ۲۱ میلیون سکه برسد. به خاطر همین آهنگ نشر نزولی، بیت‌کوین به عنوان یک ارز *ضدتورم* شناخته می‌شود، چون (بر خلاف پول‌های معمولی) نمی‌توان بیشتر از آهنگ انتشار تعیین‌شده در الگوریتم‌های پروتکل بیت‌کوین پول جدید «چاپ کرد».

بیت‌کوین در پشت صحنه نام یک پروتکل، یک شبکه‌ی همتا-به-همتا، و یک نوآوری در پردازش توزیع‌شده نیز هست. در واقع، بیت‌کوین به عنوان یک پول دیجیتال فقط اولین کاربرد این اختراع بوده است. بیت‌کوین حاصل به بار نشستن چندین دهه پژوهش در حوزه‌های رمزنگاری و سیستم‌های توزیع‌شده است و خود نیز چهار نوآوری کلیدی در بر دارد که به گونه‌ای منحصر به فرد و قدرتمند با یکدیگر ترکیب شده‌اند. بیت‌کوین از چهار بخش زیر تشکیل شده است:

- یک شبکه‌ی همتا-به-همتای غیرمتمرکز (پروتکل بیت‌کوین)
- یک دفتر کل تراکُنش عمومی (بلاک‌چین)
- مجموعه‌ای از قواعد برای اعتبارسنجی مستقل و نشر پول (قواعد اجماع)
- ساز و کاری برای دستیابی به اجماع غیرمتمرکز جهانی روی بلاک‌چین معتبر (الگوریتم اثبات-کار)

به عنوان یک برنامه‌نویس، من بیت‌کوین را همانند پول اینترنتی، و شبکه‌ای برای مبادله‌ی ارزش و تثبیت مالکیت دارایی‌های دیجیتال از طریق پردازش توزیع‌شده می‌بینم. اما بیت‌کوین مانند یک کوه یخ است که در نگاه اول فقط بخش بسیار کوچکی از آن به چشم می‌آید.

این فصل را با تشریح مفاهیم و اصطلاحات اصلی بیت‌کوین شروع کرده، سپس نرم‌افزارهای مورد نیاز را معرفی می‌کنیم، و در آخر طرز استفاده از بیت‌کوین برای انجام یک تراکُنش ساده را نشان می‌دهیم. از فصل بعد شروع به باز کردن لایه‌های این فناوری می‌کنیم و ساز و کار داخلی شبکه و پروتکل بیت‌کوین را بررسی خواهیم کرد.

پول دیجیتال قبل از بیت‌کوین

ظهور عملی پول دیجیتال ارتباط تنگاتنگی با پیشرفت رمزنگاری دارد. وقتی به چالش‌های بنیادی مبادله‌ی بیت‌های دیجیتال با کالا و خدمات نظر بیندازیم، این ارتباط نزدیک چندان هم جای تعجب نخواهد بود. برای هر کسی که بخواهد از پول دیجیتال برای خرید و فروش کالا و خدمات استفاده کند، سه پرسش اساسی پیش می‌آید:

۱. آیا می‌توان اطمینان داشت این پول اصل بوده و تقلبی نیست؟
۲. آیا می‌توان مطمئن بود این پول دیجیتال فقط یک بار می‌تواند خرج شود (مسأله‌ی خرج دوباره)؟
۳. آیا می‌توان اطمینان داشت کس دیگری نمی‌تواند مدعی مالکیت این پول شود؟

مسئولان سیاسی-اقتصادی کشورها با تولید کاغذهای غیرقابل‌جعل و فناوری‌های پیشرفته‌ی چاپ اسکناس به طور پیوسته در حال مبارزه با تقلب و جعل اوراق بهادار هستند. پول فیزیکی مشکل دوم را ندارد چون یک برگ اسکناس (یا سکه) نمی‌تواند در آن واحد در دو مکان حضور داشته باشد. البته، امروزه پول سنتی اغلب به صورت دیجیتال ذخیره شده و جابجا می‌شود. در مورد پول سنتی، مسأله‌ی تقلب و خرج دوباره را می‌توان با تسویه‌ی تراکُنش‌های دیجیتال از طریق مجاری صلاحیت‌دار که بر گردش پول نظارت عالیه دارند، مدیریت کرد. اما در پول دیجیتال که امکان استفاده از کاغذ و مرکب ویژه یا نوار هولوگرافی وجود ندارد، رمزنگاری می‌تواند مبنایی برای اطمینان از مشروعیت ادعای مالکیت فرد بر پول باشد. به طور خاص، امضاهای دیجیتال رمزنگاری‌شده به کاربر اجازه می‌دهند یک دارایی یا تراکُنش دیجیتال را امضا کرده و مالکیت خود بر آن دارایی را اثبات کند. امضاهای دیجیتال، با معماری مناسب، همچنین می‌توانند به حل مسأله‌ی خرج دوباره کمک کنند.

وقتی در اواخر دهه‌ی ۱۹۸۰ شناخت دانشمندان علوم کامپیوتر از رمزنگاری توسعه یافت و روش‌های رمزنگاری در دسترس همگان قرار گرفت. بسیاری از پژوهشگران شروع به استفاده از رمزنگاری برای ایجاد ارزهای دیجیتال کردند. این پروژه‌های اولیه منجر به انتشار انواعی از پول دیجیتال شد که معمولاً از پشتوانه‌ی یک ارز ملی یا فلزات گرانبها مثل طلا برخوردار بودند.

هر چند ارزهای دیجیتال اولیه در عمل با موفقیت همراه بودند، ولی آنها همگی متمرکز بودند و در نتیجه دولت‌ها و جاعلان (نفوذگران) به راحتی می‌توانستند به این ارزها حمله کنند. ارزهای دیجیتال اولیه، درست مثل سیستم بانکی سنتی، از یک مرکز پایاپای مرکزی برای تسویه‌ی تراکُنش‌ها در فواصل منظم استفاده می‌کردند. متأسفانه، در اکثر موارد این ارزهای دیجیتال نوپا هدف حمله‌ی دولت‌های وحشت‌زده قرار گرفتند و به تدریج از صفحه‌ی روزگار محو شدند؛ برخی از آنها نیز با ورشکسته شدن شرکت مادر سقوط کردند. برای مقاومت در برابر دخالت رقبا، خواه دولت‌های قانونی یا عناصر تبهکار، به یک ارز دیجیتال غیرمتمرکز نیاز بود که نتوان از یک نقطه‌ی واحد به آن حمله کرد. بیت‌کوین چنین سیستمی است: یک طراحی غیرمتمرکز، و بدون نیاز به هر گونه مرجع قدرت یا نقطه‌ی کنترل مرکزی که بتوان به آن حمله کرد یا امکان بروز فساد در آن وجود داشته باشد.

تاریخچه‌ی بیت‌کوین

بیت‌کوین در سال ۲۰۰۸ با انتشار مقاله‌ای با عنوان «بیت‌کوین: یک سیستم نقدینگی الکترونیک همتا-به-همتا» نوشته‌ی فرد یا گروهی با نام مستعار *ساتوشی ناکاموتو* اختراع شد (سند https://bitcoin.org/bitcoin.pdf را ببینید). ناکاماتو با ترکیب چندین اختراع پیشین، مانند b-money و HashCash، یک سیستم نقدینگی الکترونیک کاملاً غیرمتمرکز که به هیچ مرجع مرکزی برای نشر پول یا تسویه‌حساب و اعتبارسنجی تراکُنش‌ها متکی نیست، خلق کرد. نوآوری کلیدی ناکاموتو استفاده از یک سیستم پردازش توزیع‌شده (موسوم به الگوریتم «اثبات-کار») است که در هر ۱۰ دقیقه یک «انتخابات» جهانی برگزار می‌کند و اجازه می‌دهد تا این شبکه‌ی غیرمتمرکز به یک اجماع (consensus) درباره‌ی وضعیت تراکُنش‌ها برسد. این روش *مشکل خرج-دوباره* که در آن فرد می‌تواند یک واحد پول را دو (یا چند) بار خرج کند، به گونه‌ای بدیع و زیبا حل می‌کند. پیش از بیت‌کوین، مسأله‌ی خرج-دوباره یکی از نقاط ضعف همه‌ی پول‌های دیجیتال بود که مقابله با آن از طریق تسویه‌ی تمامی تراکُنش‌ها در یک اتاق پایاپای مرکزی انجام می‌گرفت.

شبکه‌ی بیت‌کوین در سال ۲۰۰۸ بر اساس یک پیاده‌سازی مرجع که توسط ناکاموتو منتشر شد و از آن زمان تاکنون توسط برنامه‌نویسان زیادی مورد بازنگری و اصلاح قرار گرفته است، شروع به کار کرد. در طول این سال‌ها توان مورد نیاز برای پیاده‌سازی الگوریتم اثبات-کار (Proof-of-Work) [به آن استخراج (mining) هم گفته می‌شود] که امنیت و چابکی بیت‌کوین را فراهم می‌آورد، به طور نمایی افزایش یافته و امروزه توان پردازشی آن از مجموع قوی‌ترین ابرکامپیوترهای دنیا نیز پیشی گرفته است. ارزش کل بازار بیت‌کوین در مقاطعی (بسته به نرخ برابری بیت‌کوین-به-دلار) از ۲۳۰ میلیارد دلار هم فراتر رفته است. بزرگترین تراکُنش در شبکه‌ی بیت‌کوین تا به امروزه ۲۵۰ میلیون دلار بوده است که به صورت لحظه‌ای و بدون پرداخت هیچ گونه کارمزدی پردازش شده است.

در آوریل ۲۰۱۱ ساتوشی ناکاموتو از مجامع عمومی بیت‌کوین خارج شد و مسئولیت توسعه‌ی آتی این شبکه را به یک گروه از داوطلبان موفق و رو به رشد سپرد. هویت واقعی فرد یا گروه پشت پرده‌ی ابداع و توسعه‌ی بیت‌کوین همچنان ناشناخته باقی مانده است. با این حال، نه ناکاموتو نه هیچ کس دیگر کنترلی بر سیستم بیت‌کوین ندارند، چون اساس این سیستم بر اصول شفاف ریاضی، کُدهای منبع باز، و اجماع بین تمامی شرکت‌کنندگان قرار گرفته است. اختراع بیت‌کوین [صرفنظر از ارزش اقتصادی آن] به خودی خود یک پیشرفت بزرگ محسوب می‌شود، و به پیدایش و شکوفایی مباحث جدید علمی در حوزه‌های مختلف از جمله پردازش توزیع‌شده، اقتصاد و اقتصادسنجی کمک کرده است.

راه‌حلی برای یکی از مسائل پردازش توزیع‌شده

اختراع ساتوشی ناکاموتو همچنین راه‌حلی جدید و عملی برای یکی از مشکلات مشهور در حوزه‌ی پردازش توزیع‌شده، موسوم به «مسأله‌ی سرداران بیزانس»، نیز هست. به طور خلاصه، این مسأله به موضوع چگونگی تلاش برای مبادله‌ی اطلاعات در یک محیط غیرقابل‌اطمینان و بالقوه پُرخطر برای دستیابی به توافق بر سر انجام یک عمل یا حالت یک سیستم می‌پردازد. راه‌حل ساتوشی ناکاموتو، که از مفهوم اثبات-کار برای رسیدن به اجماع بدون [نیاز به] یک مرجع قابل اعتماد مرکزی استفاده می‌کند، پیشرفتی خیره‌کننده در پردازش توزیع‌شده است و کاربردهای گسترده‌ای فراتر از پول دیجیتال دارد. برای مثال، از این روش می‌توان برای اجماع بر سر صحت انتخابات، قرعه‌کشی، اَسناد رسمی، گواهی محضری دیجیتال و غیره استفاده کرد.

کاربردهای بیت‌کوین، کاربران آن، و داستان آنها

بیت‌کوین یک نوآوری در فناوری باستانی پول است. پول، در اساسی‌ترین تعریف، تسهیل‌کننده‌ی مبادله‌ی ارزش بین افراد است. بنابراین، برای درک بهتر بیت‌کوین و کاربردهای آن بهتر است این پول را از نگاه کاربران آن بررسی کنیم. در سرتاسر کتاب افرادی را خواهیم دید که با بیت‌کوین معامله می‌کنند، پس اجازه دهید به اختصار با داستان آنها و کاری که قرار است با بیت‌کوین انجام دهند، آشنا شویم.

خرده‌فروشی

آلیس در منطقه‌ی ساحلی شمال کالیفرنیا زندگی می‌کند. او از دوستش (که به کارهای فنی وارد است) چیزهایی درباره‌ی بیت‌کوین شنیده و می‌خواهد استفاده از آن را شروع کند. ما هم با آلیس در مسیر آشنایی بیشتر با بیت‌کوین، به دست آوردن مقداری از این پول، و خرج کردن آن (برای خرید یک فنجان قهوه از مغازه‌ی باب) همراه می‌شویم. داستان آلیس ما را با نرم‌افزارهای بیت‌کوین، تسعیر این ارز دیجیتال، و تراکُنش‌های پایه از دیدگاه یک مشتری خرده‌فروشی آشنا می‌کند.

عمده‌فروشی

کارول در سان‌فرانسیسکو (شمال کالیفرنیا) یک نگارخانه دارد و از خریداران تابلوهای نقاشی گرانقیمت خود بیت‌کوین نیز قبول می‌کند. در داستان کارول با خطراتی که یک حمله‌ی اجماع «۵۱٪» برای معامله‌گران عمده‌ی بیت‌کوین در بر دارد، آشنا خواهید شد.

قراردادهای خارجی

باب (صاحب همان مغازه‌ی قهوه‌فروشی در منطقه‌ی ساحلی شمال کالیفرنیا) در حال راه‌اندازی یک سایت وب جدید برای کسب و کار خود است. او برای این کار با گوپش، یک برنامه‌نویس هندی ساکن بنگلور (هندوستان)، قرارداد بسته است. گوپش قبول کرده دستمزد خود را با بیت‌کوین دریافت کند. در داستان باب و گوپش با قراردادهای خارجی و نقل و انتقال بین‌المللی بیت‌کوین آشنا می‌شوید.

فروشگاه اینترنتی

گابریل یک نوجوان کارآفرین در ریودوژانیرو (برزیل) است که در فروشگاه اینترنتی کوچک خود لوازمی مانند پیراهن، لیوان و برچسب با آرم بیت‌کوین (Ƀ) می‌فروشد. از آنجا که گابریل به سن قانونی نرسیده، نمی‌تواند حساب بانکی داشته باشد؛ ولی والدینش مشوق اصلی او در ادامه دادن به این مسیر کارآفرینی هستند، پس لازم است راهی برای دریافت/پرداخت پول پیدا کند.

امور خیریه

اوژنی مدیر یک مؤسسه‌ی خیریه کودکان در فیلیپین است. او که به تازگی با بیت‌کوین آشنا شده، می‌خواهد از امکانات آن برای گسترش فعالیت‌های جمع‌آوری کمک‌های خیریه در داخل و خارج از کشور، و همچنین تسریع در توزیع این کمک‌ها و رساندن آنها به مناطق نیازمند استفاده کند. در این داستان با کاربرد بیت‌کوین در امور خیریه در سطح بین‌المللی آشنا خواهید شد.

واردات/صادرات

محمد یک واردکننده‌ی لوازم الکترونیکی در دوبی (امارات متحده‌ی عربی) است که تلاش می‌کند با استفاده از بیت‌کوین به فرآیند پرداخت بهای اقلام وارداتی از کشورهای مختلف (مثل چین و ایالات متحده) سرعت ببخشد. در داستان محمد با کاربرد بیت‌کوین در معاملات عمده‌ی بین‌المللی آشنا می‌شوید.

استخراج بیت‌کوین

جینگ یک دانشجوی کامپیوتر در شانگهای (چین) است. او که از درآمد بیشتر بدش نمی‌آید، با استفاده از مهارت‌های خود در مهندسی کامپیوتر یک سیستم برای استخراج بیت‌کوین (که می‌توان آن را «چاه بیت‌کوین» نامید) بر پا کرده است. در داستان جینگ بیت‌کوین را از دیدگاه «صنعتی» بررسی می‌کنیم: آشنایی با ابزارهای تخصصی که برای امن کردن شبکه‌ی بیت‌کوین و انتشار پول جدید به کار می‌روند.

همه‌ی این داستان‌ها بر اساس نمونه‌های واقعی ساخته شده‌اند، افراد و شرکت‌هایی که در حال ایجاد بازارهای جدید برای بیت‌کوین هستند، و برای مشکلات اقتصاد جهانی راه‌حل‌های مبتکرانه‌ای ارائه می‌کنند.

از کجا باید شروع کرد؟

بیت‌کوین یک *پروتکل* است که به کمک برنامه‌ی کاربردی مناسب (برنامه‌ای که به زبان همان پروتکل صحبت کند) می‌توان با آن ارتباط برقرار کرد. یکی از رایج‌ترین برنامه‌ها برای ارتباط با سیستم بیت‌کوین کیف‌پول بیت‌کوین (bitcoin wallet) است، درست مثل مرورگر وب که محبوب‌ترین ابزار ارتباط با پروتکل HTTP است. همان طور که برای انتخاب مرورگر وب گزینه‌های زیاد پیش رو دارید (اینترنت اکسپلورر، کروم، سافاری، فایرفاکس)، انواع بسیار زیادی از کیف‌پول بیت‌کوین در بازار وجود دارد. و درست همان طور که بعضی مرورگرها را دوست داریم و از بعضی دیگر متنفریم، انواع مختلف کیف‌پول بیت‌کوین نیز از نظر کیفیت، کارایی، امنیت، حفظ حریم خصوصی کاربر، و قابل اطمینان بودن با یکدیگر متفاوت هستند. پروتکل بیت‌کوین دارای یک پیاده‌سازی مرجع، معروف به «مشتری ساتوشی» یا «هسته‌ی بیت‌کوین»، است که از پیاده‌سازی اولیه‌ی نوشته‌شده توسط ساتوشی ناکاموتو مشتق شده و یک کیف‌پول هم دارد.

انتخاب کیف‌پول بیت‌کوین

سرعت رشد و تکامل هیچ یک از بخش‌های زیست‌بوم بیت‌کوین به اندازه‌ی کیف‌پول آن زیاد نبوده است. رقابت در این بخش بسیار شدید است، و در حالی که ممکن است در همین لحظه یک کیف‌پول جدید در حال ورود به بازار باشد، دوره‌ی فعالیت تعداد زیادی از کیف‌پول‌هایی که سال گذشته معرفی شده‌اند، عملاً به آخر رسیده است. برخی کیف‌پول‌ها برای یک پلتفرم و کاربران خاص عرضه شده‌اند، برخی دیگر برای افراد تازه‌کار مفید هستند، در حالی که کیف‌پول‌های دیگر با امکانات و ویژگی‌های متعدد کاربران حرفه‌ای را هدف گرفته‌اند. انتخاب کیف‌پول تا حد زیادی سلیقه‌ای است و به نیازها و تخصص کاربر بستگی دارد، به همین دلیل پیشنهاد یک کیف‌پول (یا پروژه‌ی) خاص تقریباً غیرممکن است. با این حال، می‌توانیم با دسته‌بندی کیف‌پول‌های موجود بر حسب پلتفرم و کارکرد آنها، تا حدی در انتخاب یک کیف‌پول مناسب به شما کمک کنیم. از آن بهتر این که جابجایی پول بین کیف‌پول‌های بیت‌کوین آسان، ارزان و سریع است، بنابراین می‌توانید با خیال راحت چند تا از آنها را امتحان کرده و سپس کیف‌پولی را که با نیازهای شما سازگارتر است، انتخاب کنید.

کیف‌پول‌های بیت‌کوین را می‌توان بر حسب پلتفرم به صورت زیر دسته‌بندی کرد:

کیف‌پول میز کار

این اولین نوع از کیف‌پول‌های بیت‌کوین بود که به عنوان یک مرجع پیاده‌سازی ایجاد شد و اکثر کاربران بیت‌کوین به خاطر ویژگی‌های متنوع، خودکار بودن و کنترلی کاملی که بر دارایی‌های بیت‌کوین به آنها می‌دهد، از این کیف‌پول استفاده می‌کنند. با این حال، اجرای این کیف‌پول روی سیستم‌عامل‌های متداول (مثل ویندوز و Mac OS) معایب امنیتی خاص خود را خواهد داشت چون این سیستم‌ها اغلب پیکربندی مناسبی نداشته و ناامن هستند.

کیف‌پول موبایل

رایج‌ترین کیف‌پول بیت‌کوین. اجرای این کیف‌پول روی پلتفرم‌های تلفن هوشمند متداول (مثل آندروید و iOS) بهترین گزینه برای کاربران تازه‌کار است. اغلب این کیف‌پول‌ها ساده هستند و کاربری آسانی دارند، ولی کیف‌پول‌های قدرتمندتر و با امکانات کامل نیز برای کاربران پیشرفته‌تر در بازار وجود دارد.

کیف‌پول وب

کیف‌پول‌هایی که از طریق مرورگر وب کار می‌کنند و (درست مثل وب‌میل) در یک سرویس‌دهنده‌ی شخص-ثالث نگهداری می‌شوند. برخی از این کیف‌ها دارای یک برنامه‌ی سمت-مشتری هستند که به کاربر اجازه می‌دهد کنترل

کلیدهای بیت‌کوین خود را کاملاً در دست داشته باشد، ولی اکثر آنها (در ازای راحتی کاربر) کنترل کلیدهای بیت‌کوین را خوددر دست می‌گیرند. ذخیره کردن مقادیر زیاد بیت‌کوین در این قبیل سرویس‌دهنده‌های شخص-ثالث توصیه نمی‌شود.

کیف‌پول سخت‌افزاری

این نوع از کیف‌پول دستگاه کوچکی است که یک برنامه‌ی امن برای ذخیره کردن بیت‌کوین روی آن اجرا می‌شود. این دستگاه‌ها معمولاً از طریق رابط USB یا NFC (ارتباط-فاصله‌ی-نزدیک) با کامپیوتر یا تلفن هوشمند کار می‌کنند. این کیف‌پول‌ها که تمام عملیات مدیریت بیت‌کوین را روی یک سخت‌افزار تخصصی انجام می‌دهند، امن‌ترین نوع کیف‌پول تلقی می‌شوند و برای ذخیره کردن مقادیر زیاد بیت‌کوین مناسب هستند.

کیف‌پول کاغذی

همان طور که گفتیم، کلیدهای بیت‌کوین رشته‌های کاراکتری متشکل از حروف و ارقام هستند که می‌توان آنها را چاپ کرد. وقتی کلیدهای بیت‌کوین را روی کاغذ (یا هر ماده‌ی دیگری مثل چوب یا فلز) چاپ می‌کنید و آنها را نگه می‌دارید، به آن کیف‌پول کاغذی می‌گویند. کیف‌پول کاغذی از نظر فناوری چندان پیشرفته نیست ولی بسیار امن است (به خصوص برای ذخیره‌سازی بلندمدت بیت‌کوین). به ذخیره‌سازی آفلاین بیت‌کوین اغلب *انباره‌ی سرد* هم گفته می‌شود.

روش دیگر دسته‌بندی کیف‌پول‌های بیت‌کوین بر اساس میزان خودمختاری و چگونگی برهم‌کُنش آنها با شبکه‌ی بیت‌کوین است:

مشتری گره-کامل

مشتری کامل، یا گره کامل (full node)، به یک مشتری گفته می‌شود که تاریخچه‌ی کامل تراکُنش‌های بیت‌کوین (تمام تراکُنش‌هایی که توسط تمامی کاربران صورت گرفته) را ذخیره کرده، کیف‌پول کاربر را مدیریت می‌کند، و می‌تواند به طور مستقیم آغازگر تراکُنش‌ها روی شبکه‌ی بیت‌کوین باشد. یک گره کامل تمام جنبه‌های پروتکل بیت‌کوین را خودش مدیریت کرده و کل بلاک‌چین و هر تراکُنش انجام‌شده را به طور مستقل اعتبارسنجی می‌کند. یک مشتری گره کامل به منابع سخت‌افزاری قابل‌توجهی نیاز دارد (بیش از ۱۲۵ GB فضای هارد دیسک، و ۲ GB حافظه)، ولی کاملاً خودمختار است و در اعتبارسنجی تراکُنش‌ها مستقل عمل می‌کند.

مشتری سبک‌وزن

مشتری سبک‌وزن، که به آن مشتری «اعتبارسنجی پرداخت ساده» (SPV) نیز گفته می‌شود، برای دسترسی به اطلاعات تراکُنش‌های بیت‌کوین به گره‌های کامل (به پاراگراف قبل نگاه کنید) متصل می‌شود، ولی کیف‌پول کاربر را به صورت محلی ذخیره کرده، و تراکُنش‌ها را خودش اعتبارسنجی و ارسال می‌کند. مشتری سبک‌وزن به طور مستقیم و بدون واسطه با شبکه‌ی بیت‌کوین برهم‌کُنش می‌کند.

مشتری API شخص-ثالث

این نوع مشتری به جای اتصال مستقیم به شبکه‌ی بیت‌کوین از طریق یک سیستم ثالث از توابع API (رابط برنامه‌نویسی برنامه‌های کاربردی) با این شبکه برهم‌کُنش می‌کند. کیف‌پول این مشتری می‌تواند نزد خود کاربر یا در یک سرویس‌دهنده‌ی ثالث ذخیره شده باشد، ولی تمامی تراکُنش‌ها از طریق سیستم شخص-ثالث انجام می‌گیرند.

با ترکیب این دسته‌بندی‌ها می‌توان انواع زیادی از کیف‌پول ایجاد کرد، ولی اغلب کیف‌پول‌های بیت‌کوین در سه دسته‌ی رایج جای می‌گیرند: مشتری کامل میز کار، کیف‌پول سبک‌وزن موبایل، و کیف‌پول وب شخص-ثالث. از آنجا که اغلب کیف‌پول‌ها می‌توانند روی پلتفرم‌های مختلف اجرا شوند و همچنین می‌توانند به روش‌های مختلفی با شبکه‌ی بیت‌کوین برهم‌کُنش داشته باشند، مرز میان آنها اغلب مبهم و نامشخص است.

برای پوشش طیف وسیع خوانندگان این کتاب، ما طرز استفاده از تعدادی مشتری‌های بیت‌کوین موجود در بازار، از پیاده‌سازی مرجع آن (هسته‌ی بیت‌کوین) گرفته تا کیف‌پول‌های موبایل و وب، را نشان خواهیم داد. برای اجرای برخی از این مثال‌ها به هسته‌ی بیت‌کوین نیاز خواهید داشت؛ هسته‌ی بیت‌کوین علاوه بر آن که می‌تواند یک مشتری کامل باشد، دارای توابع API برای دسترسی به سرویس‌های کیف‌پول، شبکه‌ی بیت‌کوین و تراکُنش نیز هست. اگر علاقه دارید با رابط برنامه‌نویسی سیستم بیت‌کوین آشنا شوید، باید هسته‌ی بیت‌کوین (یا یکی از دیگر مشتری‌های آن) را اجرا کنید.

یک شروع سریع

آلیس (که در قسمت قبل با او آشنا شدیم) هیچ سررشته‌ای از امور فنی ندارد و فقط به تازگی وصف بیت‌کوین را از دوستش شنیده است. دوست آلیس، جو، در یک مهمانی چنان با اشتیاق درباره‌ی بیت‌کوین حرف می‌زند که آلیس می‌پرسد چطور می‌تواند استفاده از آن را شروع کند. جو می‌گوید بهترین نقطه‌ی شروع برای کاربران تازه‌وارد نصب یک کیف‌پول موبایل است، و چند تا از کیف‌پول‌های مورد علاقه‌ی خود را به او توصیه می‌کند. آلیس هم کیف‌پول مایسلیوم (Mycelium) برای اَندروید را از اینترنت گرفته و در گوشی تلفن هوشمند خود نصب می‌کند.

وقتی آلیس برای اولین بار مایسلیوم را اجرا می‌کند، این برنامه (مانند اغلب کیف‌پول‌های بیت‌کوین دیگر) به طور خودکار یک کیف‌پول جدید برای او ایجاد می‌سازد. کیف‌پول جدید آلیس چیزی شبیه شکل ۱-۱ است.

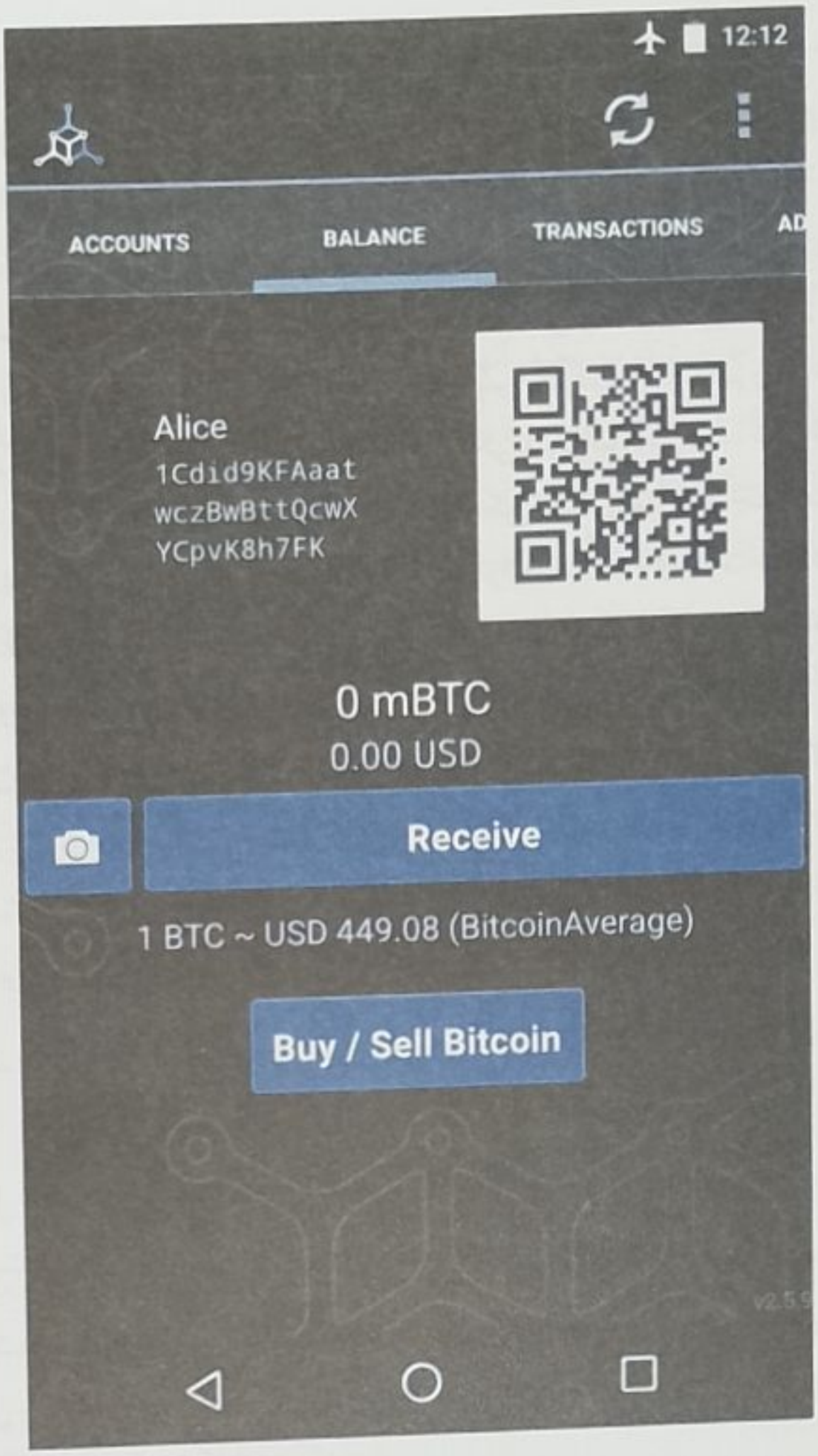
هشدار

به این آدرس بیت‌کوین نفرستید، چون برای همیشه آن را از دست خواهید داد!

مهم‌ترین بخش این تصویر *آدرس بیت‌کوین* آلیس است، همان رشته‌ی بلندی که از تعداد زیادی حرف و رقم تشکیل شده: `1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK`. در کنار این آدرس بیت‌کوین یک کُد QR می‌بینید، از آن کُدهایی که می‌توان با دوربین تلفن هوشمند آنها را اسکن کرد و اطلاعات دورن آنها را خواند. آلیس می‌تواند این آدرس یا کُد QR را با لمس کردن آنها، یا لمس کردن دکمه‌ی Receive، در حافظه‌ی موقت گوشی خود ذخیره کند. در اکثر کیف‌پول‌ها وقتی کُد QR را لمس کنید، بزرگنمایی آن بیشتر می‌شود تا راحت‌تر بتوانید آن را با دوربین گوشی‌های دیگر اسکن کنید.

توجه

آدرس‌های بیت‌کوین رقم با ۱ یا ۳ شروع می‌شوند. این آدرس‌ها را می‌توانید (درست مثل آدرس ایمیل) به دیگران بدهید تا از آن برای ارسال مستقیم بیت‌کوین به کیف‌پول شما استفاده کنند. از نظر امنیتی، هیچ اطلاعات حساسی در این آدرس‌ها وجود ندارد و می‌توان آنها را به همگان اعلام کرد. هیچ محدودیتی از نظر داشتن آدرس‌های بیت‌کوین وجود ندارد و می‌توانید به هر تعداد دلخواه آدرس بیت‌کوین داشته باشید که همگی به کیف‌پول شما منتهی می‌شوند. در حقیقت، بسیاری از برنامه‌های کیف‌پول جدید (برای تأمین بیشترین محرمانگی) به ازای هر تراکُنش یک آدرس جدید ایجاد می‌کنند. همان طور که قبلاً هم گفته‌ایم، یک کیف‌پول چیزی نیست جز مجموعه‌ای از آدرس‌های بیت‌کوین و کلیدهایی که می‌توان قفل آنها را باز کرد.



شکل ۱-۱ کیف‌پول موبایل مایسلیوم.

پس از نصب کیف‌پول و ایجاد آدرس بیت‌کوین، اکنون آلیس آماده‌ی دریافت بیت‌کوین است. این برنامه‌ی کیف‌پول به ازای هر آدرس بیت‌کوین یک کلید خصوصی تصادفی نیز تولید می‌کند. اما تا این لحظه آدرس آلیس هنوز در هیچ کجای سیستم بیت‌کوین «ثبت» نشده و برای شبکه‌ی بیت‌کوین شناخته‌شده نیست. این آدرس بیت‌کوین فقط عددی است متناظر با یک کلید خصوصی که آلیس می‌تواند از آن برای کنترل دسترسی به موجودی کیف‌پول خود استفاده کند. برنامه‌ی کیف‌پول این آدرس را به طور مستقل و بدون هر گونه ارتباط با سرویس‌های ثبت‌نام تولید کرده است. در واقع، در اکثر کیف‌پول‌ها، هیچ ارتباطی بین این آدرس بیت‌کوین و اطلاعات هویتی قابل استناد کاربر وجود ندارد. تا زمانی که این آدرس در دفتر کل بیت‌کوین به عنوان گیرنده‌ی یک تراکُنش ثبت نشود، آدرس بیت‌کوین آلیس چیزی جز یک آدرس از میان میلیاردها آدرس معتبر بیت‌کوین نخواهد بود. فقط وقتی این آدرس با یک تراکُنش مرتبط شود، به بخشی از آدرس‌های شناخته‌شده در شبکه‌ی بیت‌کوین تبدیل خواهد شد.

آلیس اکنون آماده‌ی استفاده از کیف‌پول بیت‌کوین جدید خود است.

به دست آوردن اولین بیت‌کوین

اولین و دشوارترین قدم برای هر کاربر جدید به دست آوردن چند بیت‌کوین است. بر خلاف ارزهای سنتی، بیت‌کوین را نمی‌توان از بانک‌ها یا صرافی‌های معمولی خرید.

تراکُنش‌های بیت‌کوین *برگشت‌ناپذیر* هستند. اغلب سیستم‌های نقل و انتقال پول (حواله‌های بانکی یا خرید و فروش با کارت اعتباری) برگشت‌پذیر هستند. اما برگشت‌پذیر بودن معاملات می‌تواند برای فروشندگان بیت‌کوین بسیار پُرخطر باشد، چون اگر خریدار بعد از دریافت بیت‌کوین پرداخت خود را پس بگیرد، فروشنده ضرر خواهد کرد. برای کاهش این خطر، شرکت‌هایی که در ازای فروش بیت‌کوین حواله‌های الکترونیکی سنتی قبول می‌کنند، معمولاً قبل از انتقال بیت‌کوین هویت و اعتبار حساب بانکی وی را احراز می‌کنند (فرآیندی که ممکن است چند روز یا چند هفته طول بکشد). به عنوان یک کاربر جدید، این بدان معنا است که برای خرید بیت‌کوین نمی‌توانید بلافاصله از کارت‌های اعتباری یا سایر روش‌های پرداخت الکترونیک استفاده کنید. با این حال، با کمی صبر و خلاقیت نیازی هم به آن نخواهید داشت.

در اینجا چند روش خرید بیت‌کوین برای کاربران جدید را معرفی می‌کنیم:

- از یکی از دوستانتان که بیت‌کوین دارد، مقداری بیت‌کوین بخرید. اکثر کاربران بیت‌کوین از همین جا شروع کرده‌اند. این روش از همه ساده‌تر است و کمترین پیچیدگی را دارد. اگر می‌خواهید بدانید چه کسانی در شهر یا محله‌ی شما بیت‌کوین دارند و با آنها ملاقات کنید، می‌توانید عضو یکی از انجمن‌های محلی بیت‌کوین شوید؛ اکثر این انجمن‌ها در سایت وب meetup.com فهرست شده‌اند.
- برای پیدا کردن یک فروشنده‌ی نقدی بیت‌کوین در شهر یا منطقه‌ی خود از سرویس‌هایی مثل localbitcoins.com استفاده کنید.
- یک کالا (مثل دوچرخه‌ی دست دوم) یا خدمت (مانند آرایشگری یا برنامه‌نویسی) برای فروش عرضه کنید و در ازای آن بیت‌کوین بگیرید.
- اگر در شهر شما دستگاه خودپرداز بیت‌کوین وجود دارد، از آن بیت‌کوین بخرید. این ماشین‌ها پول نقد گرفته و بیت‌کوین را به کیف‌پول شما واریز می‌کنند. برای یافتن نزدیک‌ترین خودپرداز بیت‌کوین به سایت وب coinatmradar.com مراجعه کنید.
- از یک صرافی بیت‌کوین خرید کنید. امروزه در بسیاری از کشورهای دنیا صرافی‌هایی وجود دارند که بیت‌کوین هم خرید و فروش می‌کنند. برای دیدن نرخ تسعیر بیت‌کوین با پول کشور خود به سایت‌هایی مانند bitcoinaverage.com مراجعه کنید.

توجه

یکی از مزایای بیت‌کوین نسبت به دیگر روش‌های پرداخت این است که (وقتی به درستی استفاده شود) محرمانگی بسیاری بیشتری برای کاربر به ارمغان می‌آورد. به دست آوردن، نگهداری و خرج کردن بیت‌کوین نیازی به ارائه‌ی اطلاعات حساس یا شخصی ندارد. با این حال، وقتی نوبت به مبادله‌ی بیت‌کوین با پول‌های سنتی می‌رسد، اغلب گریزی از قوانین کشوری و بین‌المللی نیست. وقتی از یک صرافی بیت‌کوین می‌خرید، باید اوراق هویتی و اطلاعات حساب بانکی خود را ارائه کنید. توجه داشته باشید که به محض ایجاد ارتباط بین هویت کاربر با یک آدرس بیت‌کوین، تمامی تراکُنش‌های دیگر وی نیز قابل شناسایی و ردیابی خواهند شد. این یکی از دلایلی است که اکثر کاربران بیت‌کوین ترجیح می‌دهند از حساب‌های بانکی مخصوصی که به کیف‌پول آنها مرتبط نیست، استفاده کنند.

آلیس بعد از آشنایی با روش‌های خرید بیت‌کوین، تصمیم می‌گیرد مقداری بیت‌کوین از همان دوستش، جو، بخرد. در قسمت بعد خواهیم دید آلیس چگونه می‌تواند این کار را انجام دهد، و جو چگونه این بیت‌کوین را به کیف‌پول آلیس می‌فرستد.

مظنه‌ی روز بیت‌کوین چند است؟

قبل از این که آلیس بتواند از جو بیت‌کوین بخرد، آنها باید بر سر *نرخ تبدیل* (تسعیر) بیت‌کوین به پول رایج خود (در اینجا دلار آمریکا) توافق کنند. اینجا یک پرسش بزرگ پیش می‌آید: «چه کسی قیمت (نرخ تبدیل) بیت‌کوین را تعیین می‌کند؟» پاسخ کوتاه این است که قیمت بیت‌کوین توسط *بازار* تعیین می‌شود.

بیت‌کوین هم مانند اکثر ارزهای دیگر دارای یک *نرخ تبدیل شناور* است، یعنی مظنه‌ی بیت‌کوین بسته به میزان عرضه و تقاضا در بازار نوسان می‌کند (بالا یا پایین می‌رود). قیمت لحظه‌ای بیت‌کوین معمولاً آخرین قیمتی است که بیت‌کوین با یک پول مشخص (مانند دلار آمریکا) مبادله شده است. به عبارت دیگر، این قیمت می‌تواند در هر ثانیه دهها بار نوسان کند. سرویس‌های اعلام قیمت بیت‌کوین قیمت‌های لحظه‌ای را از بازارهای مختلف جمع‌آوری کرده و بعد از محاسبه‌ی میانگین حجمی-وزنی آنها، این میانگین را به عنوان مظنه‌ی بیت‌کوین (مثلاً، BTC/USD) اعلام می‌کنند. مظنه‌ی بیت‌کوین را می‌توان از صدها سایت وب و برنامه‌ی کاربردی به دست آورد، که در اینجا به برخی از معروف‌ترین آنها اشاره می‌کنیم:

سایت https://bitcoinaverage.com

سایتی که میانگین حجمی-وزنی بیت‌کوین را به ازای ارزهای مختلف نمایش می‌دهد.

سایت https://coincap.io

یک سرویس اعلام قیمت که نرخ لحظه‌ای بیت‌کوین (و صدها ارز رمزبنیان دیگر) را در کنار حجم معاملات آنها نمایش می‌دهد.

سایت http://bit.ly/cmebrr

یک نرخ مرجع که توسط بورس تجارت و سرمایه‌گذاری شیکاگو اعلام می‌شود، و می‌توان از آن به عنوان مرجع قراردادهای سازمانی استفاده کرد.

علاوه بر این سایت‌ها و برنامه‌های اعلام قیمت، اکثر کیف‌پول‌های بیت‌کوین می‌توانند بیت‌کوین را به طور خودکار (با نرخ روز) به ارزهای دلخواه دیگر تبدیل کنند. جو هم قبل از ارسال بیت‌کوین به آلیس از همین ویژگی کیف‌پول خود برای تبدیل بیت‌کوین به دلار استفاده می‌کند.

ارسال و دریافت بیت‌کوین

آلیس تصمیم گرفته در قدم اول خیلی خطر نکند و فقط ۱۰ دلار بیت‌کوین بخرد. پس ۱۰ دلار نقد به جو می‌دهد، در گوشی خود برنامه‌ی کیف‌پول مایسلیوم خود را باز می‌کند و دکمه‌ی Receive را انتخاب (لمس) می‌کند. با این کار، کیف‌پول مایسلیوم آلیس اولین آدرس بیت‌کوین او را به صورت کُد QR به وی نشان می‌دهد. پس از آن جو در کیف‌پول خود دکمه‌ی Send را انتخاب می‌کند. اکنون جو (فرستنده‌ی بیت‌کوین) باید دو چیز را برای کیف‌پول خود مشخص کند:

- آدرس بیت‌کوین مقصد (گیرنده‌ی بیت‌کوین)
- مقداری که باید ارسال شود، بر حسب بیت‌کوین (BTC) یا پول رایج (در اینجا، USD)

در کیف‌پول جو، در مقابل فیلد آدرس بیت‌کوین مقصد یک آیکون کوچک به شکل کُد QR دیده می‌شود که به او اجازه می‌دهد با دوربین گوشی خود کُد QR آدرس بیت‌کوین آلیس را (که بسیار طولانی و تایپ کردن آن دشوار است) از روی گوشی او اسکن کند.

بعد از اسکن کردن کُد QR در گوشی آلیس و به دست آوردن آدرس بیت‌کوین او، جو عدد ۱۰ را در فیلد «مقدار معامله» وارد می‌کند؛ کیف‌پول جو با اتصال به یک سرویس اعلام قیمت آنلاین و گرفتن آخرین نرخ تبدیل USD/BTC، این مقدار را به بیت‌کوین تبدیل می‌کند. از آنجا که در زمان انجام این مبادله نرخ تبدیل USD/BTC ۱۰۰ بوده است، ۱۰ دلار آلیس معادل ۰٫۱۰ بیت‌کوین [یا ۱۰۰ میلی‌بیت‌کوین (mBTC)] خواهد بود؛ شکل ۱-۲ را ببینید.

قبل از زدن دکمه‌ی Send، جو یک بار دیگر آدرس گیرنده و مقدار ارسال را کنترل می‌کند تا احیاناً اشتباهی رُخ نداده باشد؛ وقتی پای انتقال پول در میان است، همه چیز را به دقت و بارها کنترل کنید، چون تراکُنش‌های بیت‌کوین برگشت‌ناپذیر هستند. بعد از زدن دکمه‌ی Send، کیف‌پول موبایل جو یک تراکُنش ایجاد کرده و ۰٫۱۰ BTC به آدرس بیت‌کوین

شکل ۱-۲ صفحه‌ی کیف‌پول موبایل ایربیتز.

آلیس حواله می‌کند. کیف‌پول جو این تراکُنش را با کلید خصوصی او امضا خواهد کرد؛ این امضا به شبکه‌ی بیت‌کوین می‌گوید که جو انتقال مقدار تعیین‌شده به آدرس جدید آلیس را تأیید کرده است. از آنجا که تراکُنش‌های بیت‌کوین از طریق پروتکل همتا-به-همتا مخابره می‌شوند، با سرعت زیادی در شبکه‌ی بیت‌کوین منتشر خواهند شد. در کمتر از یک ثانیه، اکثر گره‌های شبکه این تراکُنش را دریافت می‌کنند و برای اولین بار آدرس بیت‌کوین آلیس را می‌بینند.

در همان حال، کیف‌پول آلیس به طور پیوسته در حال «گوش دادن» به تراکُنش‌های منتشرشده روی شبکه‌ی بیت‌کوین است و گوش به زنگ تراکُنش‌هایی است که با آدرس‌های کیف‌پول او منطبق باشند. چند ثانیه بعد از آن که کیف‌پول جو این تراکُنش را منتشر کرد، کیف‌پول آلیس متوجه می‌شود که ۰٫۱۰ BTC دریافت کرده است و آن را نشان می‌دهد.

تأییدیه

در ابتدا، آدرس [کیف‌پول] آلیس تراکُنش انجام‌شده از طرف جو را به صورت «تأییدنشده» نمایش خواهد داد. این بدان معنا است که تراکُنش مزبور در شبکه‌ی بیت‌کوین منتشر شده ولی هنوز در دفتر کل تراکُنش بیت‌کوین، موسوم به «بلاک‌چین»، ضبط نشده است. یک تراکُنش برای تأیید شدن باید در یک بلاک قرار گیرد و به بلاک‌چین اضافه شود، رویدادی که به طور متوسط هر ۱۰ دقیقه اتفاق می‌افتد. به زبان امور مالی سنتی، به این اتفاق تسویه گفته می‌شود. در فصل ۱۰ به طور مفصل درباره‌ی انتشار، اعتبارسنجی و تسویه (تأیید) تراکُنش‌های بیت‌کوین صحبت خواهیم کرد.

اکنون آلیس ۰٫۱۰ BTC بیت‌کوین به دست آورده و می‌تواند آن را خرج کند. در فصل آینده خواهید دید آلیس چگونه اولین خرید خود با بیت‌کوین را انجام می‌دهد، و در تشریح این فرآیند با فناوری‌های زیربنایی تراکُنش و انتشار بیت‌کوین بیشتر آشنا خواهید شد.