سخن ناشر

بیت‌کوین: گام نخست در رستگاری از بردگی بانک‌ها

بیت‌کوین را خواه ساتوشـــی ناکاموتو یا هر فرد یا گروه و با هر نیت و طینتی ابداع کرده باشـــند، انگشت اشارتی بود به راه رهایی بشریت از غُل و زنجیر بانک‌ها و مؤسسات مالی و اعتباری: خبری خوش برای بشریت، چه آگاهانه چه ناخودآگاه! نقل قول زیر از «سِر جوزیا استمپ» رئیس بانک مرکزی انگلستان (۱۹۲۸) در خصوص بانک و بانکدار چنان سنگین و دشنام‌گونه به نظر می‌آید که بسیاری کوشیده‌اند آن را جعلی قلمداد کنند:

> سیستم‌های بانکی از «هیچ» پول تولید می کنند! این روش شاید یکی از شگفت‌انگیزترین شعبده‌های ابداع‌شده در تاریخ بشر باشد! بانکداری در پلیدی نطفه بسته و در گناه به دنیا آمده است. بانکداران صاحب کلّ زمین شده‌اند.

حتی اگر این نقل قول را مجعول بدانیم، ولی کیست که با نگاهی به عملکرد بانک‌ها در خلال ۶۲۰ سال اخیر که به شکل مدرن فعّال هستند، تا همین امروز، چنین مضمونی را تأیید نکند و این فریب‌کاری‌ها، تبانی‌ها، اختلاس، و جعل آمار و ارقام توســـط بانک‌ها و مؤسســـات مالی/اعتباری را زندگی نکرده باشد؟ [نخستین بانک به شکل مدرن و امروزی در سال ۱۳۹۷ میلادي به نام «مدیچی» در ایتالیا بنیانگذاری شد، در حالی که بانکداری به شکل بدوی آن حدود ۵۰۰۰ هزار سال و به شکل نیمه‌مدرن حدود ۱۶۰۰ سال سابقه‌ی فعالیت دارد. ماهیت پول به عنوان یک واسطه‌ی انتقال نیز قدمتی بین ۵ تا ۷ هزار سال دارد.] بحران‌های وحشتناک مالی در سطح جهان از تاریک‌خانه‌ی بانکدارها و بورس‌بازان به سان مارهای سمّی به جان و مال مردم افتادند؛ از نمونه‌های اخیر آن می‌توان به «رکود عظیم» سال ۱۹۲۸ که به «افسردگی بزرگ» نیز مشهور است و برای قریب ۱۲ سال دامنه‌ی آن به سطح اروپا و آسیا نیز گسترش یافت و زمینه‌ساز جنگ جهانی دوم شد، یا رکود جهانی سال ۲۰۰۸ که همه به خاطر می‌آوریم، اشاره کرد که بورس‌بازان و بانکداران مسبب همه مصیبت‌های آن بودند؛ چه زندگی‌ها و رؤیاها که ویران نشد و چه مردمی که دسترنج عمرشان را نباختند. [پیشینه‌ی بحران‌های مالی و اَبَرتورم‌های ناشی از تقلب‌های سیستماتیک و هزینه‌کردهای بی‌پشتوانه به حدود ۴۰۰ سال قبل از میلاد در آتن برمی‌گردد که در نهایت به سقوط آتن به دست اسپارت‌ها انجامید. طنز تلخ تاریخ این که یونان همین امروز نیز دچار اَبَر بحران مالی است!]

کشور خود ما نیز با این بحران‌ها و فریب‌کاری‌ها بیگانه نبوده و نیست و هر روز طشت رسوایی یک مؤسسه‌ی مالی/اعتباری از بام می‌افتد و سرمایه‌های جمعی از مردم به باد فنا می‌رود، ولی باز هم در کنار آن یک مؤسسه‌ی جدید با وعده‌هایی چرب‌تر و لذیذتر افتتاح می‌شود و این دور باطل ادامه می‌یابد؛ کافی است در امتداد یک خیابان قدم بزنید؛ شاید حتی یک کتابفروشی یا ابزارفروشی پیدا نکنید ولی بی‌تردید شعبات بیشماری از بانک‌ها و مؤسسات مالی/اعتباری خواهید یافت که با عمارت‌هایی زیبا و فریبنده ورود شـــما را خوشامد می‌گویند و در ستادن اندوخته‌هایتان (به ویژه اگر ارزش آن فربه باشد)

رویی گشاده دارند؛ ولی در آن سوی ماجرا، اگر وامی طلب کنید یا اقساطی عقب‌مانده داشته باشید، دل‌پریش و رنجیده‌خاطر بیرون خواهید آمد. کوتاه‌سخن آن‌که، بانک‌ها و مؤسسات مالی/اعتباری با ساختار «متمرکز» یکی از بدکردارترین و بدنام‌ترین الزامات ناگزیر زندگی بشر امروز و دیروز بوده و هستند.

این همه مشکلات تاریخی اقتصاد از کجا منشأ می‌گیرند که عقلانیت در مبارزه با آن شکست خورده، در حالی که بشر در شاخه‌های دیگر دانش، همانند ریاضی، فیزیک، شیمی، پزشکی و علوم طبیعی، و از عمق اقیانوس‌ها تا دوردست‌های منظومه‌ی شمسی به دستاوردهایی شگفت‌انگیز رسیده است؟ پاسخ ساده است: تمرکز، عدم شفافیت، دروغ‌های اشتهاآور، و قدرتی که پول در به هم زدن هر معادله‌ای دارد! ظهور بیت‌کوین در سال ۲۰۰۸ نویدی بود بر پیروزی قریب‌الوقوع عقلانیت، البته اگر این بار به جای «گرگ‌های وال‌استریت» نهنگ‌هایش سر بر نیاورند!

ارز رمزبنیانِ بیت‌کوین پس از معرفی در سال ۲۰۰۸ مسیری بس ناهموار و پُر فراز و نشیب را طی کرده و هنوز هم برای آن‌که در نقش یک واحد پول اصیل و قابل‌اعتماد ایفای نقش کند، با مشکلات عدیده‌ای روبرو است؛ ولی بزرگ‌ترین دستاوردها و ویژگی‌های پلتفرم بیت‌کوین که باید آنها را ارج نهاد و به آینده‌ی این نوع از پول‌های رمزبنیان امیدوار بود، عبارتند از:

- دفتر کلّ عمومی که تمام تراکُنش‌های مالی در آن ثبت می‌شوند، به شکل «غیرمتمرکز» روی ماشین هر کس که مایل به مشارکت در حفظ ارزش این پول باشد، بارگذاری می‌شود و لحظه به لحظه به‌روز خواهد شد. همه‌ی افراد در این مشارکت، هم‌رده و همتا هستند و نسخه‌ی یکسانی از دفتر کلّ را در اختیار خواهند داشت و معادله‌ی «تمرکز = فساد» به هم می‌خورد.
- هیچ تراکُنش مالی از چشم مردم جهان پنهان نمی‌ماند، زیرا دفتر کلّ عمومی در اختیار هر کسی که آن را درخواست کند، قرار خواهد گرفت و حتی اگر آن شخص صاحب هیچ پولی در این سیستم نباشد، می‌تواند با بارگذاری دفتر کلّ بر روی کامپیوتر خود، پیشینه‌ی تمام تراکُنش‌ها را مشاهده و اعتبارسنجی کند.
- الگوهای تولید پول و گردش آن قانونمند و شفاف هستند، و صدور و اعتبارسنجی یکایک تراکُنش‌ها همگی بر اساس اصول مستحکم ریاضیات چنان بنا نهاده شده که در شرایط طبیعی هرگز قابل جعل، تغییر یا فریبکاری نیست. [اگر از گوشه و کنار دنیا خبرهایی از سرقت بیت‌کوین یا تقلب و دزدی و کارهای نامشروع به گوشتان رسیده است، اینها به واسطه‌ی ناآگاهی افراد و افتادن در تله‌ی نفوذگران و ضعف امنیتی سیستم‌ها است، و گر نه اصول و مبنای پلتفرم بیت‌کوین بر مبنای علم ریاضیات بنا نهاده شده و لااقل بر اساس آنچه بشر از علم ریاضیات به چنگ آورده، خدشه‌بردار نیست، مگر آن که اتفاق محیرالعقولی در دنیای ریاضیات بیفتد، مثلاً حل مسأله‌ی تجزیه‌ی اعداد بزرگ یا مسأله‌ی لگاریتم گسسته امکان‌پذیر شود.] افزون بر این، هر شخص یا گروهی می‌تواند به فراخور توان پردازشی که در اختیار دارد، در فرآیند غیرقابل‌جعل کردن تراکُنش‌ها (که فرآیندی بسیار دشوار و در بیت‌کوین مستلزم توان پردازش میلیون‌ها پردازنده‌ی موازی است) مشارکت داشته باشد و ما به ازای آن با تولید بیت‌کوین‌های جدید جایزه بگیرد.

بدین شیوه، شفافیت در روند تولید پول مانع از تزریق پول بی‌پشتوانه به سیستم پولی جهان خواهد شد؛ از سویی، آگاهی همگانی از یکایک تراکُنش‌ها و امکان اعتبارسنجی آنها توسط افراد معمولی جامعه، یک سیستم پولی غیرمتمرکز و مردم‌نهاد پدید خواهد آورد که در آن امکان اختلاس، ارائه‌ی آمار جعلی، زد و بندهای رایج و فریب‌کاری‌هایی مثل خرج-دوباره‌ی یک واحد پول به پشتوانه‌ی «عقلانیت» (علم ریاضی و زیرساخت عظیم شبکه‌ی اینترنت) لااقل از «دیدگاه نظری» ناممکن است! [فراموش نکنید که تمام پروتکل بیت‌کوین بر اساس توابعی بنیانگذاری شده که ذات ریاضی دارند.] وقتی مردم یک جامعه مطمئن شوند که با سیستمی مطمئن و شفاف طرف هستند، با خیال راحت‌تر دارایی‌ها و اندوخته‌های مالی خود را در آن نگهداری خواهند کرد. [هرچند بیت‌کوین تمام شرایط ایجاد یك سیستم پولی مردم‌نهاد را فراهم آورده، ولی چون قیمتی ثابت و پشتوانه‌ای جز مصرف انرژی الکتریکی ندارد، هنوز نتوانسته

نقش یک پول با ارزش ثابت را ایفا کند. با این حال، مبانی نظری بیت‌کوین بسیار هوشمندانه، مستحکم و امیدبخش است. بی‌تردید آینده متعلق به ارزهای رمزبنیان است، حتی اگر بیت‌کوین وجود خارجی نداشته باشد.]

فارغ از آن که موافق یا مخالف بیت‌کوین به عنوان یک پول دیجیتال فرامرزی و مردم‌نهاد باشیم، ارزش این ابداع انقلابی آن بود که یک «اثبات مفهومی» برای امکان‌پذیر بودن تحقق یک سیستم بانکی مردم‌نهاد ارائه کرد، و فقط پس از آن بود که در جهان هنگامه‌ای شگفت‌انگیز در خلق ارزهای رمزبنیان (و کاربردهای مشابه همانند قراردادهای هوشمند) به پا شد. پیش از ادامه، اجازه دهید دو مقوله را از یکدیگر تفکیک کنیم:

- بیت‌کوین بر اساس چه اصول و پروتکل‌هایی کار می‌کند، و چرا می‌تواند سه شرط یاد شده در بالا را احراز کند؟ در این خصوص ابتدا باید مفهوم و عملکرد بلاک‌چین را بشناسید. این کتاب شما را با این اصول و پروتکل‌ها آشنا می‌کند.
- آیا بیت‌کوین واقعاً به یک پول قابل‌اعتماد تبدیل شده است و باید هر چه زودتر دارایی‌های خود را از بانک‌ها و مؤسسات مالی/اعتباری متمرکز بیرون بکشیم و آنها را به بیت‌کوین یا رمزارزهای هم‌تراز تبدیل کنیم؟ آیا بیت‌کوین قادر است با ارائه‌ی پاسخی مناسب برای چالش‌ها و مشکلات کنونی سیستم‌های متمرکز، به یک پول قابل‌اعتماد تبدیل شده، و به تدریج اعتماد مردم را جلب کند و جایگزین سیستمی با هزاران سال قدمت شود و بشریت را از شرّ نهادهایی که پشت درهای بسته با دارایی‌ها و دسترنج مردم قمار می‌کنند، رهایی بخشد؟

پاسخ به پرسش اول دلیلی است برای آن که چرا باید این کتاب را خواند، با جزئیات فنی و برنامه‌نویسی آن آشنا شد، و تا حد ممکن به ریاضیات حاکم بر توابع پایه (شامل اصول رمزنگاری، دَرهم یا چکیده‌ی پیام، امضای دیجیتالی و نظایر آن) تسلط پیدا کرد. پاسخ به پرسش دوم ساده نیست و پاسخ آن را باید در علم اقتصاد جستجو کرد: بیت‌کوین موافقان و مخالفان سرشناسی دارد ولی بقا یا نابودی بیت‌کوین اهمیتی ندارد؛ آنچه اهمیت دارد همان حقیقتی است که در ابتدای این سخن به آن اشاره کردیم: اکنون دیگر می‌دانیم ایجاد پولی با پشتوانه‌ی مردمی و تراکُنش‌های شفاف و غیرقابل جعل و انکارنشدنی امکان‌پذیر شده است.

بلاک‌چین: تابش نور به ظلمت معابد دروغ

ویژگی‌های بنیادین بیت‌کوین (غیرقابل‌تغییر بودن تراکُنش‌ها، شفافیت، و همتا-به-همتا و مردم‌نهاد بودن آن) به پشتوانه‌ی بستری است که بلاک‌چین نام گرفته: در این کتاب خواهید دید که بلاک‌چین چیزی نیست جز یک ساختار ساده از بلاک‌های حاوی چندین تراکُنش (همراه با اندکی اسکریپت)، که برای آن که احدی در دنیا نتواند محتوای این بلاک‌ها را تغییر دهد، تحت فرآیندی موسوم به «اثبات-کار» که میلیون‌ها نفر در گوشه و کنار جهان در آن مشارکت دارند، یک «مسأله‌ی دشوار» طرح و سپس حل می‌شود. دلیل تغییرناپذیری بلاک‌ها آن است که هر گونه جعل و فریب‌کاری مستلزم تبانی میلیون‌ها نفر در اقصی نقاط جهان است و یافتن ائتلافی از این همه بزهکار یا دسترسی به قدرت پردازشی در حد چند میلیون پردازنده‌ی موازی در عمل ناشدنی است (مگر جاهایی که پای دولت‌های بزرگ مثل چین یا روسیه در میان باشد).

بنابراین، بلاک‌چین یک ساختمان داده از بلاک‌های حاوی تراکُنش‌های بیت‌کوین با ساختاری ساده و جهانشمول است که در قالب یک «لیست پیوندی» به یکدیگر زنجیر شده‌اند و تغییر در یک بلاک باعث خواهد شد که این رشته از محل بروز تغییر تا انتهای زنجیره از اعتبار ساقط شود. مسأله‌ی دشواری که بایستی برای اعتباردهی به بلاک‌چین حل شود، عبارت است از یافتن یک دَرهم از سرآیند بلاک که شرط خاصی را برآورده می‌کند. اگر چه برای یافتن این دَرهم به توان پردازشی وحشتناکی نیاز است، ولی خوشبختانه اعتبارسنجی آن (یعنی بررسی پاسخی که دیگران ادعای یافتن آن را دارد) بسیار ساده بوده و از عهده‌ی یک پردازنده‌ی معمولی (حتی گوشی‌های تلفن همراه) هم برمی‌آید. بلاک بعدی که به بلاک‌چین اضافه خواهد شد دَرهم سرآیند بلاک قبلی را در بطن خود دارد، بنابراین هر تغییر عمدی در یک بلاک فقط همان یک بلاک را نامعتبر نخواهد ساخت، بلکه تمامی بلاک‌های پس از آن نیز از اعتبار ساقط خواهند شد.

کتـــاب حاضر نه تنها افراد عادی را با نحوه‌ی عملکرد بیت‌کوین، مفهوم آدرس بیت‌کوین، ســـاختن کیف پول، و انتقال و تراکُنش آشنا می‌کند، بلکه جزئیات دقیق بلاک‌چین را به همراه کُدهای آموزنده شرح می‌دهد. با این رویکرد، نه تنها افرادی که ســـابقه‌ی برنامه‌نویسی ندارند، با مفهوم بیت‌کوین و بلاک‌چین آشنا می‌شوند، بلکه برنامه‌نویسان کنجکاو نیز می‌آموزند که چگونه خودشـــان درستی کُدها را به بوته‌ی آزمایش بگذارند، آنها را تغییر بدهند، وحتی با بهبود کُدها و پیشنهاد تغییرات جزئی یا کلی در بلاک‌چین، به بهینه‌سازی بلاک‌چین و بیت‌کوین کمک کنند.

در ایـــن کتاب خواهید دید کـــه چگونه می‌توان برنامه‌های لازم برای راه‌اندازی یـــک گره بیت‌کوین را نصب کرد. یکی دیگر از ویژگی‌های جذّاب کتاب حاضر که بســـیاری از مقالات و کتاب‌های دیگر به سادگی از کنار آن می‌گذرند، تشریح چگونگی عملکرد شـــبکه‌ی همتا-به-همتایی است که بلاک‌چین روی آن بارگذاری می‌شود. این بخش یکی از جذاب‌ترین بخش‌های کتاب است که مردم‌نهاد بودن بلاک‌چین و بیت‌کوین را به زبانی ساده توصیف می‌کند.

در ادامه، این کتاب شما را با مفاهیم «اجماع» و «استخراج بیت‌کوین» آشنا می‌کند و به زبانی ساده شرح می‌دهد که در سیستم بیت‌کوین چگونه مردم سرتاسر دنیا در مورد صحت و درستی تراکُنش‌های مالی و تولید بیت‌کوین‌های جدید به اجماع (توافق همگانی) می‌رسند. آشنایی با این مفهوم ذهن شما را آماده می‌کند تا در مورد پول‌های دیگری مثل «اِتریوم» که در آنها روش اجماع متفاوت است، ساده‌تر بیندیشید و قضاوت کنید. همچنین یاد خواهید گرفت که در بلاک‌چین می‌توان در هر بلاک اسکریپت‌نویسی هم کرد؛ هر چند زبان اسکریپت‌نویسی بیت‌کوین «تورینگ کامل» نیست و محدودیت‌هایی دارد. [پلتفرم اتریوم دارای یک زبان اسکریپت‌نویسی به نام Solidity است که یک ماشین تورینگ کامل است که با آن می‌توان هر نوع برنامه‌ای نوشت، ولی (برخلاف روش‌های مرسوم برنامه‌نویسی) باید برای اجرای هر اسکریپت هزینه‌ای موسوم به «گاز» بپردازید که در آن هر دستورالعمل قیمت متفاوتی دارد!!!]

در ادامـــه‌ی کتاب نکاتی در خصـــوص امنیت بیت‌کوین و بلاک‌چیـــن خواهید یافت، و در آخر هـــم می‌توانید با کاربردهای بیشتر بلاک‌چین آشنا شـــوید. جزییات پُرشمار دیگری از مفاهیم بلاک‌چین و بیت‌کوین در این کتاب توضیح داده شـــده‌اند که نام بردن از آنها در این سخن کوتاه نمی‌گنجد و بهتر است خودتان با کنجکاوی در لابلای صفحات کتاب به کند و کاو در آنها بپردازید.

و اما حرف آخر: شـــاید یکی از دستاوردهای مهم مطالعه‌ی این کتاب آن باشد که چراغی در ذهنتان روشن خواهد کرد که بلاک‌چین را (فارغ از کاربرد آن در خلق پول‌های دیجیتال مثل بیت‌کوین) به مثابه یک «بستر برنامه‌نویسی» ببینید که جنبه‌های وسیعی از دنیای فردا را تغییر خواهد داد، زیرا بلاک‌چین را می‌توان (فراتر از کاربرد آن در ایجاد بانک‌ها و مؤسسات مالی/اعتباری غیرمتمرکز و مردم‌نهاد) برای کاربردهایی مانند قراردادهای هوشمند (غیرقابل انکار)، نهادهای مرتبط با مدیریت دارایی، شرکت‌های بیمه، سیستم‌های پذیرش مسئولیت یا محول کردن آن، مؤسسات تأمین انرژی (به ویژه تولید انرژی‌های پاک توسط بخش‌های خصوصی کوچک ولی توزیع‌شده و پُرتعداد)، سیستم‌های بهداشت و درمان، صنایع مرتبط با تولید و ثبت آثار معنوی (موسیقی، فیلم، محتوی و نظایر آنها)، صیانت از آرا در انتخابات الکترونیکی، اداره‌ی ثبت احوال، دفاتر ثبت اسناد، و اینترنت اشیأ (IoT) به کار گرفت.

این کتاب را بخوانید و با خود بیندیشـــید که با امکان‌پذیر شـــدن یک پروتکل اجماع عمومی، دنیای فردا چگونه جایی خواهد بود، و شـــما چه کاربردهایی می‌توانید برای آن تصور کنید که تا پیش از ابداع بلاک‌چین از مشکلاتی مانند عدم‌شـــفافیت، تمرکزگرایی، زد و بند، جعل و تزویر، حق‌کشی و قبیله‌ســـالاری، و رانت رنج می‌برده‌اند؛ کاربردهایی که می‌توانند آرزوی دیرینه‌ی دموکراسی را به تحقق نزدیک‌تر کنند.

در پایان، امیدواریم از خواندن این کتاب هم به دانشی جدید دست یابید و هم لذّت ببرید!

انتشارات نص

پاییز ۱۳۹۸

پیش‌گفتار

نوشتن کتابی درباره‌ی بیت‌کوین

اواسط سال ۲۰۱۱ بود که اولین بار با بیت‌کوین آشنا شدم. واکُنش فوری من «پووف! پول خرخوان‌ها!» بود و آن را نادیده گرفتم؛ در واقع در همان لحظه نتوانستم متوجه اهمیت بیت‌کوین شوم. این واکُنشی است که در خیلی از افراد دیگر (حتی باهوش‌ترین کسانی که می‌شناسم) هم دیده‌ام، که قدری باعث تسکین من می‌شود. بار دوم که (در یک گروه مباحثه‌ی ایمیلی) به بیت‌کوین برخوردم، تصمیم گرفتم برای آشنایی دست اول با این پدیده، مقاله‌ی معروف ساتوشی ناکاموتو را بخوانم. هنوز لحظه‌ای که خواندن این گزارش ۹ صفحه‌ای را تمام کردم، به یاد دارم، لحظه‌ای که فهمیدم بیت‌کوین فقط یک ارز دیجیتال ساده نیست، بلکه یک شبکه‌ی اعتماد است که می‌تواند مبنایی برای بسیاری چیزهای دیگر (و نه فقط پول) باشد. فهمیدن این که بیت‌کوین «پول نیست، بلکه یک شبکه‌ی اعتماد غیرمتمرکز است»، باعث شد در چهار ماه بعدی هر چیزی از بیت‌کوین به دست رسید، ببلعم. تمام هوش و حواسم روی بیت‌کوین متمرکز شده بود؛ روزی ۱۲ ساعت (یا بیشتر) جلوی کامپیوتر می‌نشستم، می‌خواندم، یادداشت برمی‌داشتم، برنامه می‌نوشتم، و تا می‌توانستم یاد می‌گرفتم. در پایان این دوره‌ی عزلت تب‌آلود چهار ماهه، در حالی که به خاطر تغذیه‌ی نامنظم و غیراصولی ۱۰ کیلو وزن کم کرده بودم، مصمم بودم کارم را روی بیت‌کوین متمرکز کنم.

دو سال بعد، پس از راه‌اندازی چند استارت‌آپ کوچک برای پژوهش و کند و کاو در سرویس‌ها و محصولات مختلف مرتبط با بیت‌کوین، تصمیم گرفتم اولین کتابم را بنویسم. بیت‌کوین تمام ذهن مرا به خود مشغول کرده بود؛ بیت‌کوین هیجان‌انگیزترین فناوری بود که از زمان ظهور اینترنت با آن روبرو شده بودم. و اکنون زمان آن بود که شور و اشتیاقم درباره‌ی این فناوری خارق‌العاده را با دیگران در میان بگذارم.

این کتاب برای کیست؟

این کتاب به طور عمده برای برنامه‌نویسان است. اگر به یک زبان برنامه‌نویسی آشنا هستید، این کتاب طرز کار ارزهای رمزبنیان، چگونگی استفاده از آنها، و روش نوشتن برنامه برای کار با این ارزها را به شما یاد خواهد داد. البته فصل‌های ابتدایی کتاب برای کسانی که برنامه‌نویسی نمی‌دانند و فقط می‌خواهند با اصول و مبانی نظری بلاک‌چین، بیت‌کوین و ارزهای رمزبنیان آشنا شوند، نیز مناسب است.

بیت‌کوین از طبیعت الهام گرفته است!

آنهایی که با بیت‌کوین مخالف هستند، اغلب استدلال می‌کنند که بدون وجود یک نهاد مرکزی نمی‌توان چیزی به نام پول (یا اساساً اقتصاد) داشت. اما طبیعت نشان داده است که سیستم‌های غیرمتمرکز و به غایت منظم و انعطاف‌پذیر می‌توانند بدون اتکا به یک قدرت مرکزی، سلسله‌مراتب یا بخش‌های پیچیده شکل بگیرند. عالی‌ترین نمونه‌ی آن کلونی مورچه‌ها و زنبورها است. در کلونی مورچه‌های کشاورز هیچ قدرت برتر یا سلسله‌مراتبی وجود ندارد. مورچه‌های کشاورز غذای خود را از طریق پرورش نوعی قارچ روی برگ‌های خردشده‌ی گیاهان به دست می‌آورند، و اجتماع آنها به ادعای ویکیپدیا «بزرگترین و پیچیده‌ترین جامعه‌ی جانوری روی کره زمین پس از انسان» است. بله، این کلونی‌ها (که گاه تعداد اعضای آنها به میلیون‌ها مورچه می‌رسد) یک ملکه هم دارند، ولی توجه کنید که وظیفه‌ی ملکه فقط تخم گذاشتن است، و به همین دلیل مهم‌ترین عضو کلونی به شمار می‌رود، ولی این ملکه هیچ قدرت خاص یا مطلقه‌ای ندارد.

بیت‌کوین یک شبکه‌ی اعتماد غیرمتمرکز و بسیار ساخت‌یافته است که می‌تواند بسیاری از فرآیندهای مالی را پشتیبانی کند؛ با این حال، در یک شبکه‌ی بیت‌کوین هر گره فقط چند قاعده‌ی ساده‌ی ریاضی را دنبال می‌کند. این رفتار ساخت‌یافته ناشی از برهم‌کُنش بین گره‌های متعدد شبکه است، نه پیچیدگی ذاتی یا اعتماد در هر گره واحد. شبکه‌ی بیت‌کوین (مانند کلونی مورچه‌ها) یک شبکه‌ی چابک و انعطاف‌پذیر متشکل از گره‌های ساده است که قواعد ساده‌ای را دنبال می‌کنند و بدون وجود هر گونه هماهنگی مرکزی می‌توانند کارهای شگفت‌انگیزی انجام دهند.

ساختار بصری کتاب

اصطلاحات و عبارتی که برای اولین بار معرفی می‌شوند، با قلم ضخیم آبی مشخص خواهند شد، و در مواردی که لازم باشد، معادل لاتین آنها را نیز می‌آوریم. از قلم کج آبی برای تأکید بر کلمات، و عبارات مهم استفاده کرده‌ایم. کُد برنامه‌ها با قلم فاصله‌ی ثابت (monospace) آورده شده، و در مواردی که کاربر (شما) باید چیزی وارد کند، آن را با قلم فاصله‌ی ثابت ضخیم زیرخط‌دار (**monospace**) مشخص می‌کنیم. مانند همیشه در این کتاب هم از آیکون‌ها و علائم بصری خاص برای تأکید بر مفاهیم و نکات مهم و مفید استفاده شده است:

توجه مطالب این بخش‌ها به شما کمک می‌کنند کاری را بهتر یا راحت‌تر انجام دهید.

نکته در این بخش‌ها توجه شما به یک قاعده‌ی کلی جلب می‌شود.

هشدار وقتی به این بخش‌ها می‌رسید، احتیاط پیشه کنید. عدم رعایت این نکات می‌تواند باعث اشتباه یا عملکرد ناصحیح شود.

کُدهای کتاب

مثال‌های کتاب با زبان‌های C++ و پایتون نوشته شده، و با استفاده از خط-فرمان یک سیستم‌عامل شبه-یونیکس، مانند لینوکس یا MacOS، اجرا شده‌اند. این کُدها را می‌توانید (به همراه اغلب نرم‌افزارهای مورد نیاز، و بسیاری از ابزارها و مطالب مفید دیگر) در دیسک پیوست کتاب بیابید. البته کُدهای کتاب را می‌توان بدون زحمت زیاد در زبان‌های برنامه‌نویسی دیگر نیز پیاده‌سازی کرده و در سیستم‌های دیگر (مانند ویندوز) اجرا کرد. در مواردی که طول یک خط کُد از پهنای صفحه‌ی کتاب بیشتر است، در انتهای دستور یک ↵ قرار داده و ادامه‌ی آن را به خط (یا خطوط) بعد منتقل کرده‌ایم؛ این کاراکتر فقط برای چاپ کتاب است و شما باید آن را هنگام نوشتن دستورات حذف کنید و تمام دستور را در یک خط بنویسید.

تا جایی که امکان داشته، از کلیدهای رمزگذاری، مقادیر و محاسبات واقعی استفاده کرده‌ایم تا بتوانید آنها را به همان صورتی که باید باشد، اجرا کنید. تراکُنش‌ها، بلاک‌ها، و ارجاعات بلاک‌چین همگی در یک بلاک‌چین بیت‌کوین واقعی معرفی شده‌اند و بخشی از دفتر کل عمومی هستند، بنابراین می‌توانید آنها را روی هر سیستم بیت‌کوین دلخواه مشاهده کنید.

قسمت اعظم آدرس‌های بیت‌کوین، تراکُنش‌ها، کلیدها، کُدهای QR، و داده‌های بلاک‌چین به کار رفته در این کتاب واقعی هستند، یعنی می‌توانید آن بلاک‌چین را در یک مرورگر باز کنید، نگاهی به تراکُنش‌ها بیندازید، و آنها را در برنامه‌های خود بازیابی کنید. با این حال، توجه داشته باشید که کلیدهای خصوصی به کار رفته در این کتاب علنی [یا «سوزانده»] شده‌اند و دیگر قابل استفاده نیستند. به عبارت دیگر، اگر پولی به هر یک از این آدرس‌ها بفرستید، برای همیشه از جیب‌تان رفته، و شاید به حساب یکی از خوانندگان زرنگ این کتاب که از آن کلیدها استفاده کرده، واریز شده باشد!

هشدار

اگر نمی‌خواهید پول خود را از دست بدهید، **به هیچ یک از حساب‌های نشان داده شده در این کتاب پول واریز نکنید.**

فهرست