ویراست دوم

آندریاس آنتونوپولوس

دکتر احسان ملکیان
(عضو هیئت علمی دانشگاه خوارزمی)

مهندس علیرضا زارع‌پور

همه چیز درباره‌ی

بیت کوین

برنامه نویسی برای بلاک چین باز

همه چیز درباره‌ی رمزارز

بیت کوین

ویرایش دوم

برنامه‌نویسی برای بلاک‌چین باز

تولید و استخراج/ کاربرد و کارایی آن در تجارت و کسب و کار

نویسنده

آندریاس آنتونوپولوس

مترجمان

دکتر احسان ملکیان

(عضو هیأت علمی دانشگاه خوارزمی)

مهندس علیرضا زارع‌پور

ناشر کتب مهندسی، کامپیوتر، دانشگاهی، مدیریت

نص

سرشناسه	: آنتونوپولوس، آندریاس ام.	Antonopulos, Andreas M.
عنوان و نام پدیدآور	: همه چیز درباره‌ی بیت‌کوین برنامه‌نویسی برای بلاک‌چین باز / نویسنده آندریاس آنتونوپولوس؛ مترجم احسان ملکیان، علیرضا زارع‌پور.	
مشخصات نشر	: تهران: نشر نص، ۱۳۹۸.	
مشخصات ظاهری	: ۳۱۶ ص: مصور.	
شابک	: 978 -964- 410- 393- 3	
وضعیت فهرست‌نویسی	: فیپا	
یادداشت	: عنوان اصلی: Mastering Bitcoin: programming the open blockchain, 2nd ed, 2017 .	
موضوع	: بیت‌کوین	
موضوع	: Bitcoin	
موضوع	: انتقال الکترونیکی وجوه - - برنامه‌های کامپیوتری	
موضوع	: Electronic funds transfers -- Computer programs	
موضوع	: بازرگانی الکترونیکی -- برنامه‌های کامپیوتری	
موضوع	: Electronic commerce -- Computer programs	
موضوع	: پول -- برنامه‌های کامپیوتری	
موضوع	: Money -- Computer programs	
شناسه افزوده	: ملکیان، احسان، ۱۳۵۰-، مترجم	
شناسه افزوده	: زارع‌پور، علیرضا، ۱۳۴۰-، مترجم	
رده‌بندی کنگره	: HG ۱۷۱۰	
رده‌بندی دیویی	: ۳۳۲/۴۲	
شماره کتابشناسی ملی	: ۵۸۱۴۰۱۳	

موسسه علمی فرهنگی

همه چیز درباره‌ی بیت‌کوین (برنامه‌نویسی برای بلاک‌چین باز)

نویسنده: آندریاس آنتونوپولوس

مترجمان: دکتر احسان ملکیان (عضو هیأت علمی دانشگاه خوارزمی)، مهندس علیرضا زارع‌پور

ویراستار: حسین زارع مهرجردی

چاپ اول: پاییز ۱۳۹۸

تیراژ: ۱۰۰۰

ناشر: نص

طراحی، آماده سازی: نص

قیمت: ۷۹۰۰۰ تومان

دفتر انتشارات: تهران، م. انقلاب، نبش خ. منیری جاوید، ساختمان بهمن طبقه‌ی اول

تلفن: ۶۶۴۱۲۳۸۵ - ۶۶۴۶۵۶۷۴ - ۶۶۹۵۳۸۸۳

فروشگاه: ضلع جنوب شرقی م. انقلاب، شماره ۲۵ تلفن: ۶۶۴۰۵۳۷۲ و ۳-۶۶۹۷۵۲۹۲

شابک: ۳ - ۳۹۳ - ۴۱۰ - ۹۶۴ - ۹۷۸

ISBN: 978 - 964 - 410 - 393 - 3

وب سایت: www.nass.ir

ایمیل: info@nass.ir

معرفی

آندریاس آنتونوپولوس

آندریاس م. آنتونوپولوس (متولد ۱۹۷۲) کارآفرین یونانی-انگلیسی و از مدافعان سرسخت بیت‌کوین است. آنتونوپولوس مدرک مهندسی کامپیوتر، ارتباطات داده و سیستم‌های توزیعی خود را از کالج لندن گرفت، و پس از آن به کار و تحقیق در زمینه‌ی امنیت کامپیوتری مشغول شد. وی علاوه بر میزبانی پادکست «بیائید از بیت‌کوین حرف بزنیم» (https://letstalkbitcoin.com/)، در دانشگاه نیکوزیا (قبرس) دوره‌ی تخصصی ارزهای دیجیتال تدریس می‌کند. آنتونوپولوس بعد ازآشنایی با بیت‌کوین در سال ۲۰۱۲، کار خود را رها کرد و به طور تمام وقت به فعالیت پژوهشی-اقتصادی در زمینه‌ی این ارز رمزبنیان مشغول شد. در ژانویه ۲۰۱۴، آنتونوپولوس به عنوان رئیس بخش امنیت Blockchain.info منصوب شد، ولی در سپتامبر همان سال این شغل را رها کرد. آنتونوپولوس با نوشتن کتاب حاضر شهرتی جهانی در دنیای بیت‌کوین برای خود دست و پا کرد، به طوری که طرفداران بیت‌کوین از سرتاسر دنیا بیش از ۱۰۰ بیت‌کوین به‌وی هدیه کردند!

علیرضا زارع‌پور

اگر دانش‌آموخته‌ی رشته‌ی کامپیوتر یا علاقمند و فعّال در این حوزه باشید، بی‌اغراق محال است در کتابخانه‌ی شخصی خود یکی از هشتاد عنوان کتاب تألیفی یا ترجمه‌ی مهندس علیرضا زارع‌پور در میان کتاب‌هایتان خودنمایی نکند. مؤلف و مترجمی که شمارگان کتاب‌هایش از نیم میلیون فراتر رفته و برخی از آثار وی بیش از ۳۰ بار تجدید چاپ شده است. وی با نخستین کتابش، «ویژوال بیسیک»، قریب به ۲۵ سال پیش (روزگارانی که این زبان دوست‌داشتنی و ساده، همانند زبان پایتون در روزگار کنونی، نیازهای برنامه‌نویسی همگان را برآورده می‌کرد) هنگامه‌ای به پا کرد و یکی از اولین تجربه‌هایش در ترجمه پانزده بار پیاپی به چاپ رسید. چند سال بعدتر نیز ترجمه‌ی کتاب شبکه‌های کامپیوتری (اثر آندروس. تانن‌بام)، بیش از سی بار تجدید چاپ شد. به جرأت می‌توان گفت که مهندس زارع‌پور سهم بسزایی در آشنایی نسل جوان این مرز و بوم با علوم و فنون رشته‌ی کامپیوتر داشته است. او یکی از نویسندگان پیشکسوت در یك حوزه‌ی انقلابی از دانش روزگار ماست و کارش را زمانی شروع کرد که زندگی اجتماعی بشر تا این اندازه تحت سیطره‌ی کاربردهای کامپیوتر نبود.

مهندس زارع‌پور فارغ‌التحصیل مهندسی برق از دانشگاه علم و صنعت ایران در سال ۱۳۷۲ است. وی به طور انحصاری با «انتشارات نص» کار می‌کند، و خوانندگان گرانمایه‌ای که به آثار ایشان علاقمندند، می‌توانند نظرات، پیشنهادها وانتقادهای خود درباره‌ی کتاب پیش رو را از طریق پُست الکترونیک zarepour@nasspub.com به اطلاع وی برسانند.

احسان ملکیان

دکتر احسان ملکیان از چهره‌های شناخته‌شده در حوزه‌ی کامپیوتر و فناوری اطلاعات (و دارنده‌ی عنوان پژوهشگر برتر سال ۱۳۷۵، سه بار برنده‌ی جشنواره‌ی «کتاب سال» و «کتاب سال دانشجویی»، و چندین و چند جایزه‌ی ملی دیگر در حوزه‌ی پژوهش، توسعه و نگارش) است. اولین کتاب وی «مهندسی اینترنت» بود که با ساختار خوب و قلمی روان به سرعت به یکی از کتاب‌های درسی معتبر دانشگاه‌های کشور تبدیل شد، و در تمامی سال‌های اخیر همواره یکی از پرفروش‌ترین کتاب‌ها در این حوزه بوده است. از دیگر کتاب‌های دکتر ملکیان می‌توان به «نفوذگری در شبکه»، «مسیریاب‌های سیسکو»، «امنیت داده»، «شبکه‌های کامپیوتری - تانن‌باوم» و «معماری کامپیوتر - پترسون، هنسی» اشاره کرد، که همگی با استقبال بسیار خوب خوانندگان مواجه شده‌اند؛ از جمله کتاب مهندسی اینترنت بیش از چهل و پنج بار، و کتاب شبکه‌های کامپیوتری بیش از سی بار تجدید چاپ شده‌اند.

دکتر ملکیان مدرک کارشناسی خود را از دانشگاه صنعتی اصفهان، کارشناسی ارشد را از دانشگاه شیراز، و دکترای خود را از دانشگاه شهید بهشتی تهران اخذ کرده است. وی در حال حاضر عضو هیأت علمی دانشگاه خوارزمی تهران (اولین مؤسسه‌ی آموزش عالی ایران با قدمت صد سال؛ تاسیس ۱۲۹۷) است و در خلال هجده سال اخیر به عنوان مدرس مهمان در دانشگاه‌های صنعتی شریف، شهید بهشتی، دانشگاه تهران، دانشگاه صنعتی امیرکبیر، دانشگاه الزهرا (س)، و در سالیان دورتر در دانشگاه آزاد اسلامی و بسیاری از مراکز آموش عالی دیگر به تدریس مشغول بوده و همچنان بر همان عهدی است که بود: «دانشجو بماند». تخصص وی شبکه‌های کامپیوتری، رمزنگاری و امنیت، و معماری کامپیوتر است، و افزون بر کارشناسی ارشد و دکترای معماری کامپیوتر، یك کارشناسی ارشد هم در حوزه‌ی هوش مصنوعی دارد.

دکتر ملکیان از پنج سال قبل در خلال تدریس درس امنیت شبکه در دانشگاه امیرکبیر به بلاک‌چین و بیت‌کوین علاقمند شد و از آن زمان تا کنون در حوزه‌ی بلاک‌چین به شکل نظری متمرکز شده و به همراهی دانشجویان ارشد و دکترای خود به فعالیت‌های بنیادین و نظری در این حوزه مشغول است و همایش‌های متعددی در زمینه‌ی رمزارزها برگزار کرده است. وی ضمن تدریس و راهنمایی دانشجویان کارشناسی ارشد و دکترا در حوزه‌ی کامپیوتر، اخیراً به کسوت دانشجو در حوزه‌ی اقتصاد نیز در آمده است.

دکتر ملکیان به صورت انحصاری با «انتشارات نص» کار می‌کند. خوانندگان گرانقدر آثار وی می‌توانند نظرات و پیشنهادهای خود درباره‌ی این کتاب را از طریق آدرس پُست الکترونیک malekian@nasspub.com یا ehsan.malekian@gmail.com با وی در میان بگذارند.

سخن ناشر

بیت‌کوین: گام نخست در رستگاری از بردگی بانک‌ها

بیت‌کوین را خواه ساتوشی ناکاموتو یا هر فرد یا گروه و با هر نیت و طینتی ابداع کرده باشند، 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 می‌کنند! 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 توسط بانک‌ها و مؤسسات 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 اَبَربحران 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 شما را خوشامد می‌گویند و در ستادن اندوخته‌هایتان (به ویژه اگر ارزش آن فربه باشد)

روی گشاده دارند؛ ولی در آن سوی ماجرا، اگر وامی طلب کنید یا اقساطی عقب‌مانده داشته باشید، دل‌پریش و رنجیده‌خاطر بیرون خواهید آمد. کوته‌سخن 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 رمزبنیان 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 قابل اعتماد 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 به‌-روز 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 غیرقابل جعل 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 یک 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 قابل اعتماد 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 قابل اعتماد 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 (غیرقابل تغییر 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 اشیا (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