



همه چیز درباره‌ی رمزارز

ویراست دوم

# بیت کوین

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 هیات علمی دانشگاه خوارزمی)

مهندس علیرضا زارع‌پور

ناشر: کتب مهندسی، کامپیوتر، دانشگاهی، مدیریت

نص

|                     |                                                                                                                                   |                            |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| سرشناسه             | : آنتونوپولوس، آندریاس ام.                                                                                                        | .Antonopoulos, Andreas M   |
| عنوان و نام پدیدآور | : همه چیز درباره‌ی بیت کوین برنامه‌نویسی برای بلاک چین باز / نویسنده آندریاس آنتونوپولوس؛ مترجم احسان ملکیان، علیرضا علیزاده پور. | : آنتونوپولوس، آندریاس ام. |
| مشخصات نشر          | : تهران: نشر نص، ۱۳۹۸.                                                                                                            |                            |
| مشخصات ظاهری        | : ۳۱۶ ص: مصور.                                                                                                                    |                            |
| شابک                | : 978-964-410-393-3                                                                                                               |                            |
| وضعیت فهرست‌نویسی   | : فیا                                                                                                                             |                            |
| یادداشت             | : عنوان اصلی: Mastering Bitcoin: programming the open blockchain, 2nd ed, 2017.                                                   |                            |
| موضوع               | : بیت کوین                                                                                                                        |                            |
| 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        | : ملک، حسن، ۱۳۵۰-، مترجم                                                                                                          |                            |
| شناسه افزوده        | : زار، حسین، علیزاده، ۱۳۴۰-، مترجم                                                                                                |                            |
| رده‌بندی گنگره      | : ۱۷۱۰                                                                                                                            |                            |
| رده‌بندی دیویی      | : ۴۳۰                                                                                                                             |                            |
| شماره کتابشناسی ملی | : ۵۸۱۰۱۳                                                                                                                          |                            |



موسسه علمی فرهنگی

همه چیز درباره‌ی بیت کوین (برنامه‌نویسی برای بلاک چین)

نویسنده: آندریاس آنتونوپولوس

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

ویراستار: حسین زارع مهرجردی

چاپ اول: پاییز ۱۳۹۸

تیراژ: ۱۰۰۰

ناشر: نص

طراحی، آماده سازی، چاپ و صحافی: موسسه علمی فرهنگی نص

قیمت با DVD: ۴۹۰۰۰ تومان

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

تلفن: ۶۶۹۵۳۸۸۳ - ۶۶۴۶۵۶۷۴ - ۶۶۴۱۲۳۸۵

فروشگاه: ضلع جنوب شرقی م. انقلاب، شماره ۲۵ تلفن: ۵۳۷۲۰۶۶۴ و ۶۶۹۷۵۲۹۲-۳

ISBN: 978-964-410-393-3

شابک: ۳-۳۹۳-۴۱۰-۹۶۴-۹۷۸

وب سایت: www.nass.ir

ایمیل: info@nass.ir

## پیش‌گفتار

### نوشتن کتابی درباره‌ی بیت‌کوین

اواسط سال ۲۰۱۱ میلادی که اولین بار با بیت‌کوین آشنا شدم. واکنش فوری من «پوف! پول خر خوان‌ها!» بود و آن را نادیده گرفتم؛ در واقع در همان لحظه من به‌طور مستقیم متوجه اهمیت بیت‌کوین نشوم. این واکنشی 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 برخورد کردم، 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 رسد را به‌طور عمیق و کامل یاد بگیرم. تمام هوش و حواسم روی بیت‌کوین متمرکز شده بود؛ روزی ۱۲ ساعت (یا بیشتر) جلوی کامپیوتر می‌نشستم، می‌خواندم، یادداشت بر می‌داختم، 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 کار 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 غیر متمرکز 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 ویکپدیا «بزرگترین و پیچیده‌ترین جامعه‌ی جانوری روی کره زمین پس از انسان» است. بله، این کلونی‌ها (که ۲۰۰ تا ۳۰۰ میلیارد مورچه‌ها را در بر می‌گیرد) یک ملکه هم دارند، ولی توجه کنید که وظیفه‌ی ملکه فقط تخم‌گذاری است، و به همین دلیل مهم‌ترین عضو کلونی به شمار می‌رود، ولی این ملکه هیچ قدرت خاص یا مطلقه‌ای ندارد.

بیت‌کوین یک شبکه‌ی غیر متمرکز و بسیار سخت‌یافته 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 برهم‌دوش شدن گره‌های متعدد شبکه است، نه پیچیدگی ذاتی یا اعتماد در هر گره واحد. شبکه‌ی بیت‌کوین (مانند کلونی مورچه‌ها) یک شبکه‌ی جابک 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 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 کرب (کد) باید چیزی وارد کند، آن را با قلم فاصله‌ی ثابت ضخیم زیرخط‌دار (monospace) مشخص می‌کنیم. مانند همه در این کتاب هم از آیکون‌ها و علائم بصری خاص برای تأکید بر مفاهیم و نکات مهم و مفید استفاده شده است:

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

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

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

## کدهای کتاب

مثال‌های کتاب با زبان‌های C++ و پایتون نوشته شده، و با استفاده از خط-فرمان یک سیستم عامل شبه-یونیکس، مانند لینوکس یا MacOS، اجرا شده‌اند. این کدها را می‌توانید (به همراه اغلب نرم‌افزارهای مورد نیاز، و بسیاری از ابزارها و مطالب مفید دیگر) در دیسک پیوست کتاب بیابید. البته کدهای 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 کد 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. تراکنش‌ها، بلاک‌ها، و ارجاعات بلاک چین همگی در یک بلاک چین بیت‌کوین واقعی معرفی شده‌اند و بخشی از دفتر کل عمومی هستند، بنابراین می‌توانید آنها را روی هر سیستم بیت‌کوین دلخواه مشاهده کنید.

قسمت اعظم آن‌ها بیت‌کوین، تراکنش‌ها، کلیدها، کدهای QR، و داده‌های بلاک چین به کار رفته در این کتاب واقعی هستند، یعنی می‌توانید آن بلاک چین را در یک مرورگر باز کنید، نگاهی به تراکنش‌ها بیندازید، و آنها را در برنامه‌های خود بازبایی 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 دیگر این کتاب که از آن کلیدها استفاده کرده، واریز شده باشد!

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

هشدار