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 قابل‌استفاده 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

واژه‌نامه

در ایـــن واژه‌نامه اصطلاحات و واژه‌های مرتبط با بیت‌کوین را توضیح داده‌ایم. از آنجا که در تمام طول کتاب به کرات با این اصطلاحات مواجه خواهید شد، بهتر است از قبل با آنها آشنا شوید.

آدرس

address

یک آدرس بیت‌کوین رشته‌ای از حروف و ارقام، و چیزی شبیه `1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV`، است. آدرس‌های بیت‌کوین در واقع کلیدهای عمومی ۱۶۰-بیتی با کُدگذاری Base58Check هستند. درست همان طور که از دیگران می‌خواهید به آدرس ایمیل شما ایمیل بفرستند، هنگام دریافت یک بیت‌کوین باید از آنها بخواهید آن را به یکی از آدرس‌های بیت‌کوین شما ارسال کنند.

بیپ

BIP

پیشنهاد بهسازی بیت‌کوین. مجموعه‌ای از پیشنهادات که اعضای جامعه‌ی بیت‌کوین برای بهبود آن ارائه می‌کنند. برای مثال، BIP-21 پیشنهادی برای بهبود ساختار URI بیت‌کوین است.

بیت‌کوین

bitcoin

نام این واحد پول (سکه)، شبکه و نرم‌افزار.

بلاک

block

یک گروه از تراکُنش‌ها که با یک برچســـب زمانی و اثر انگشت از بلاک قبلی علامتگذاری شده است. برای تولید اثبات کار و معتبرسازی تراکُنش‌ها، سرآیند این بلاک دَرهم می‌شود. بلاک‌های معتبر با اجماع شبکه به بلاک‌چین اصلی اضافه می‌شوند.

بلاک‌چین

blockchain

فهرستی از بلاک‌های معتبر، که هر یک به بلاک قبلی خود و از آنجا به بلاک زاینده متصل شده‌اند.

مسأله‌ی سرداران بیزانس *Byzantine Generals Problem*

یک سیستم کامپیوتری قابل‌اطمینان باید بتواند از کار افتادن یا خرابی یک یا چند بخش خود را تحمل کند. یک عضو خراب معمولاً رفتاری از خود بروز می‌دهد [مثلاً، ارسال اطلاعات متناقض به بخش‌های مختلف سیستم]، که اغلب نادیده گرفته می‌شود. به موضوع تحمل این نوع خرابی «مسأله‌ی سرداران بیزانس» گفته می‌شود.

پایگاه‌سکه *coinbase*

یک فیلد ویژه که به عنوان تنها نقطه‌ی ورودی برای تراکُنش‌های پایگاه‌سکه به کار می‌رود. پایگاه‌سکه اجازه می‌دهد فرد جایزه‌ی بلاک را تصاحب کند و تا سقف ۱۰۰ بایت در آن داده‌ی دلخواه بنویسد. «پایگاه‌سکه» را نباید با «تراکُنش پایگاه‌سکه» اشتباه گرفت.

تراکُنش پایگاه‌سکه *coinbase transaction*

اولین تراکُنش در یک بلاک. این تراکُنش که همیشه توسط یک معدنچی ایجاد می‌شود، شامل یک پایگاه‌سکه‌ی واحد است. «تراکُنش پایگاه‌سکه» را نباید با «پایگاه‌سکه» اشتباه گرفت.

انباره‌ی سرد *cold storage*

نگه داشتن یک اندوخته‌ی بیت‌کوین به صورت آفلاین. با ایجاد کلیدهای خصوصی بیت‌کوین و ذخیره کردن آنها در یک محیط اَمن آفلاین می‌توان یک انباره‌ی سرد به وجود آورد. انباره‌ی سرد برای کسانی که صاحب دارایی‌های بیت‌کوین هستند، اهمیت بسیار زیادی دارد. کامپیوترهای آنلاین همیشه در معرض حمله‌ی نفوذگران هستند و نباید به عنوان محل نگهداری مقادیر زیاد بیت‌کوین به کار روند.

سکه‌های رنگی *colored coins*

یک پروتکل منبع باز بیت‌کوین ویرایش 2.0 که به برنامه‌نویسان اجازه می‌دهد با بهره‌گیری از کارکردهای غیرپولی بلاک‌چین بیت‌کوین، بر روی این بستر دارایی‌های دیجیتال تولید کنند.

تأییدیه *confirmation*

همین که یک تراکُنش در یک بلاک پذیرفته شود، یک تأییدیه به دست می‌آورد. به محض آن که بلاک دیگری در همان بلاک‌چین استخراج شود، این تراکُنش دارای دو تأییدیه خواهد شد، و به همین ترتیب الی‌آخر. برای آن که یک تراکُنش غیرقابل‌برگشت شود، شش تأییدیه‌ی اثبات (یا بیشتر) کافی تلقی می‌شود.

اجماع *consensus*

زمانی که چندین گره، معمولاً اکثر گره‌های شبکه، همگی بلاک‌های مشابهی در «بهترین بلاک‌چین با اعتبار محلی» خود داشته باشند. نباید آن را با «قواعد اجماع» اشتباه گرفت.

قواعد اجماع *consensus rules*

قواعد اعتبارسنجی بلاک که گره‌های کامل برای پایبندی به اجماع با گره‌های دیگر دنبال می‌کنند. نباید آن را با «اجماع» اشتباه گرفت.

دشواری *difficulty*

یک سنجه (معیار) در سرتاسر شبکه که میزان محاسبات مورد نیاز برای تولید یک «اثبات-کار» را کنترل می‌کند.

هدف‌گذاری مجدد دشواری
difficulty retargeting

محاسبه‌ی مجدد دشواری در سرتاسر شبکه که هر ۲۰۱۶ بلاک یک بار اتفاق می‌افتد و اساس آن بر توان محاسباتی لازم برای دَرهم‌سازی ۲۰۱۶ بلاک قبلی است.

هدف دشواری
difficulty target

یک سطح دشواری که در آن برای یافتن یک بلاک با به‌کارگیری تمام توان پردازشی شبکه حدود ۱۰ دقیقه زمان لازم باشد.

خرج دوباره
double spending

وضعیتی که در آن بتوان مقداری پول را بیش از یک بار با موفقیت خرج (مصرف) کرد. بیت‌کوین با ارزیابی هر تراکُنش اضافه‌شده به بلاک‌چین برای اطمینان از این که ورودی‌های آن تراکُنش قبلاً خرج نشده‌اند، مانع از بروز خرج دوباره می‌شود.

الگوریتم امضای دیجیتال منحنی بیضوی
ECDSA

الگوریتم امضای دیجیتال منحنی بیضوی (Elliptic Curve Digital Signature Algorithm) الگوریتم رمزنگاری مورد استفاده در بیت‌کوین که تضمین می‌کند هیچ کس به جز مالک حقیقی یک بیت‌کوین قادر به خرج کردن آن نیست.

کارمزد
fee

فرستنده‌ی یک تراکُنش اغلب بابت پردازش تراکُنش درخواستی خود مقداری حق‌الزحمه به شبکه پرداخت می‌کند. حداقل کارمزد اکثر تراکُنش‌ها ۰٫۵ mBTC (نیم میلی‌بیت‌کوین) است.

انشعاب
fork

وقتی دو یا چند بلاک ارتفاع یکسانی داشته باشند و در بلاک‌چین شکاف ایجاد کنند، انشعاب (که به آن انشعاب تصادفی نیز گفته می‌شود) اتفاق می‌افتد.

بلاک زاینده
genesis block

اولین بلاک در یک بلاک‌چین، که برای آغازگری ارز رمزبنیان به کار می‌رود.

انشعاب سخت
hard fork

یک واگرایی (جدایی) دائمی از بلاک‌چین اصلی (که به آن «تغییر انشعاب-سخت» نیز گفته می‌شود)؛ معمولاً هنگامی رُخ می‌دهد که گره‌های غیرارتقایافته نتوانند بلاک‌های ایجادشده توسط گره‌های ارتقایافته را که از قواعد اجماع جدیدتر پیروی می‌کنند، اعتبارسنجی کنند. نباید آن را با «انشعاب»، «انشعاب نرم»، «انشعاب نرم‌افزاری» یا «انشعاب گیت» اشتباه گرفت.

کیف‌پول سخت‌افزاری
hardware wallet

نوع خاصی از کیف‌پول بیت‌کوین که در آن کلیدهای خصوصی کاربر در یک دستگاه سخت‌افزاری اَمن ذخیره می‌شوند.

دَرهم (چکیده) ***hash***

اثر انگشت دیجیتالی یک ورودی باینری.

قفل دَرهم ***hashlock***

نوعی مانع که تا علنی (عمومی) شدن یک قطعه‌ی خاص داده جلوی خرج کردن یک خروجی را می‌گیرد. ویژگی سودمند قفل‌های دَرهم این است که به محض باز شدن (علنی شدن) یک قفل دَرهم، هر قفل دَرهم دیگری که با همان کلید بسته (اَمن) شده باشد، نیز باز خواهد شد. این ویژگی اجازه می‌دهد تا چندین خروجی با یک قفل دَرهم بسته شده و همگی به طور همزمان باز (قابل خرج کردن) شوند.

پروتکل HD ***HD protocol***

پروتکل ایجاد و انتقال کلید قطعی-سلسله‌مراتبی (Hierarchical Deterministic) [BIP-32]، که اجازه می‌دهد کلیدهای فرزند به گونه‌ای سلسله‌مراتبی از یک کلید مادر (بذر) ساخته شوند.

کیف‌پول HD ***HD wallet***

کیف‌پولی که از پروتکل ایجاد و انتقال کلید قطعی-سلسله‌مراتبی (HD) [BIP-32]، استفاده می‌کند.

بذر کیف‌پول HD ***HD wallet seed***

یک مقدار بالقوه-کوتاه که به عنوان بذر برای تولید کلید خصوصی اصلی و کُد زنجیری اصلی برای یک کیف‌پول HD به کار می‌رود. (به آن ریشه‌ی کیف‌پول HD نیز گفته می‌شود.)

قرارداد قفل-زمانی دَرهم‌شده ***HTLC***

قرارداد قفل-زمانی دَرهم‌شده (Hashed TimeLock Contract) به یک کلاس از پرداخت‌ها گفته می‌شود که از قفل-دَرهم و قفل-زمانی برای مجبور کردن گیرنده‌ی پرداخت به تصدیق دریافت آن مبلغ قبل از انقضای یک موعد مقرر (ضرب‌العجل) استفاده می‌کند. گیرنده باید در بازه‌ی زمانی مشخص‌شده اثبات رمزنگاری پرداخت را تولید کند، در غیر این صورت توانایی تصاحب مبلغ پرداختی را از دست می‌دهد و آن مبلغ به پرداخت‌کننده برگردانده می‌شود.

مشتری خود را بشناس ***KYC***

مشتری خود را بشناس (Know Your Customer) عبارت است از فرآیند یک کسب و کار برای شناسایی و اعتبارسنجی مشتریان خود. این اصطلاح برای اشاره به مقررات بانکی حاکم بر این قبیل فعالیت‌ها نیز به کار می‌رود.

انباره‌ی LevelDB ***LevelDB***

یک انباره‌ی کلید-مقدار دیسک-محور منبع باز. LevelDB یک کتابخانه‌ی سبک-وزن تک-منظوره و بسیار مستحکم است که می‌تواند با بسترهای زیادی کار کند.

شبکه‌ی آذرخش ***Lightning Network***

یک پیاده‌سازی پیشنهادی برای قراردادهای قفل-زمانی دَرهم‌شده (HTLC) با کانال‌های پرداخت دو-طرفه که اجازه می‌دهد پرداخت‌ها به طور اَمن از طریق چندین کانال پرداخت همتا-به-همتا مبادله شوند. بدین ترتیب

می‌توان شـــبکه‌ای ایجاد کرد که در آن هر همتا بتواند با همتاهای دیگر مبادله و پرداخت انجام دهد، حتی اگر بین آنها کانال باز مستقیم وجود نداشته باشد.

زمان قفل *Locktime*

زمان قفل، یا به بیان دقیق‌تر `nLocktime`، بخشی از یک تراکُنش است که زودترین زمان (یا زودترین بلاک) را که این تراکُنش می‌تواند به بلاک‌چین اضافه شود، مشخص می‌کند.

مخزن حافظه *mempool*

مخـــزن حافظه‌ی بیت‌کوین به مجموعـــه‌ی تمام داده‌های تراکُنـــش در یک بلاک که توســـط گره‌های بیت‌کوین اعتبارسنجی شده ولی هنوز تأیید نشده‌اند، گفته می‌شود.

ریشه‌ی مرکل *merkle root*

گره ریشه‌ی یک درخت مرکل، که نتیجه‌ی [دَرهم‌سازی] تمامی جفت‌های دَرهم‌شده در این درخت است. سرآیند هر بلاک باید شامل یک ریشه‌ی مرکل نتیجه‌شده از تمامی تراکُنش‌ها در آن بلاک باشد.

درخت مرکل *merkle tree*

درخت ساخته شده از دَرهم‌سازی داده‌های جفت‌شده (برگ‌ها)، و سپس جفت کردن و دَرهم‌سازی نتایج تا رسیدن به یک نتیجه‌ی واحد، که همان ریشـــه‌ی مرکل اســـت. در بیت‌کوین، برگ‌ها تقریباً همیشه تراکُنش‌های یک بلاک واحد هستند.

معدنچی *miner*

یک گره شبکه که از طریق دَرهم‌سازی متوالی، اثبات کار معتبر برای بلاک‌های جدید جستجو می‌کند.

چندامضایی *multisignature*

وقتی برای تصویب (تنفیذ) یک تراکُنش بیت‌کوین به بیش از یک کلید نیاز باشد.

شبکه *network*

یک شـــبکه‌ی همتا-به-همتا که تراکُنش‌ها و بلاک‌ها را بین تمامی گره‌های بیت‌کوین متصل به آن شـــبکه منتشر می‌کند.

نونس (رشته‌ی تصادفی) *nonce*

یک فیلد ۳۲-بیتی (۴-بایتی) در یک بلاک بیت‌کوین که مقدار آن به گونه‌ای تعیین می‌شود که این بلاک همیشه حاوی دنباله‌ای از صفرهای پیشـــرو باشد. ممکن است سایر فیلدهای بلاک تعریف دیگری داشته باشند و در این فرآیند تغییر نکنند.

تراکُنش برون-زنجیره *off-chain transaction*

جابجایی مقادیر خارج از بلاک‌چین. در حالی که تراکُنش‌های درون-زنجیره [که به ســـادگی به آنها تراکُنش گفته می‌شود] باعث تغییر بلاک‌چین می‌شوند و برای تعیین اعتبار خود به بلاک‌چین مربوطه وابسته هستند، یک تراکُنش برون-زنجیره برای ثبت و اعتبارسنجی به روش‌های دیگر متکی است.

عملگر
opcode

عملگر یا کُدهای اجرایی (operation code) در زبان «اسکریپت» بیت‌کوین که (در اسکریپت‌های کلید عمومی یا امضا) برای ارسال داده یا انجام یک عمل به کار می‌روند.

پروتکل دارایی باز
Open Assets protocol

یک پروتکل ساده و قدرتمند که روی بلاک‌چین بیت‌کوین ساخته شده و اجازه می‌دهد کاربران دارایی‌های خود را عرضه و جابجا کنند. پروتکل دارایی باز یک فَرگشت از مفهوم سکه‌های رنگی است.

عملگر OP_RETURN
OP_RETURN

آپ‌کُد مورد استفاده در یکی از خروجی‌های یک تراکُنش OP_RETURN. نباید آن را با «تراکُنش OP_RETURN» اشتباه گرفت.

تراکُنش OP_RETURN
OP_RETURN transaction

نوعی تراکُنش که از هسته‌ی بیت‌کوین 0.9.0 به بعد به طور پیش‌فرض برای انجام معاملات و استخراج بیت‌کوین به کار می‌رود. این نوع تراکُنش با اضافه کردن داده‌های دلخواه به یک اسکریپت کلید عمومی (به وضوح) غیرقابل‌مصرف اجبار گره‌های کامل شبکه به ذخیره کردن آنها در پایگاه داده‌ی UTXO خود را از بین می‌برد. نباید آن را با «آپ‌کُد OP_RETURN» اشتباه گرفت.

بلاک یتیم
orphan block

بلاک‌هایی که بلاک مادر آنها توسط گره محلی پردازش نشده، و بنابراین هنوز نمی‌توان آنها را به طور کامل اعتبارسنجی کرد.

تراکُنش یتیم
orphan transaction

تراکُنشی که به دلیل فقدان یک یا چند تراکُنش ورودی نمی‌تواند وارد مخزن تراکُنش شود.

خروجی
output

خروجی تراکُنش، یا TxOut، دو فیلد دارد: فیلد مقدار برای تعیین تعداد ساتوشی‌هایی که باید انتقال یابند، و اسکریپت کلید عمومی که شرایط لازم برای خرج کردن این ساتوشی‌ها را مشخص می‌کند.

اسکریپت P2PKH
P2PKH

تراکُنش‌هایی که یک آدرس بیت‌کوین پرداخت می‌کنند، حاوی یک اسکریپت P2PKH (پرداخت-به-دَرهم-کلیدعمومی: Pay-To-PubKey-Hash) هستند. خروجی قفل شده با اسکریپت P2PKH فقط می‌تواند با ارائه‌ی یک کلید عمومی و یک امضای دیجیتال تولید شده با کلید خصوصی متناظر آن باز (خرج) شود.

تراکُنش P2SH
P2SH

تراکُنش «پرداخت-به-دَرهم-اسکریپت» (Pay-to-Script-Hash) یک نوع تراکُنش جدید و قدرتمند است که استفاده از اسکریپت‌های تراکُنش پیچیده را تا حدی زیادی ساده می‌کند. در یک تراکُنش P2SH دیگر خبری

از اسکریپت پیچیده‌ای که شرایط خرج کردن خروجی را با جزئیات زیاد توصیف می‌کند (موسوم به اسکریپت وصول)، در اسکریپت قفل‌کننده نیست و به جای آن در اسکریپت قفل‌کننده فقط یک دَرهم از این اسکریپت گنجانده می‌شود.

آدرس *P2SH*

P2SH address

دَرهم ۲۰-بایتی یک اسکریپت که به روش Base58Check کُدگذاری شده است. آدرس‌های P2SH از پیشوند ویرایش «5» استفاده می‌کنند که بعد از کُدگذاری Base58Check منجر به تولید آدرس‌هایی خواهد شد که با کاراکتر «3» شروع می‌شوند. آدرس‌های P2SH پیچیدگی تراکُنش‌ها را از دید کاربر پنهان می‌کنند، و کاربر هنگام پرداخت دیگر اسکریپت قفل‌کننده‌ی پیچیده را نخواهد دید.

تراکُنش *P2WPKH*

P2WPKH

امضای یک تراکُنش «پرداخت-به-دَرهم-کلید-عمومی-شاهد» (Pay-to-Witness-Public-Key-Hash) حاوی همان اطلاعات تراکُنش (خرج کردن) P2PKH است، با این تفاوت که به جای فیلد «شاهد» (witness) در فیلد «امضای اسکریپت» (scriptSig) قرار می‌گیرد. فیلد «کلید عمومی اسکریپت» (scriptPubKey) آن نیز متفاوت است.

تراکُنش *P2WSH*

P2WSH

تفاوت تراکُنش «پرداخت-به-دَرهم-اسکریپت-شاهد» (Pay-to-Witness-Script-Hash) با P2SH در تغییر فیلد اثبات رمزنگاری از فیلد «امضای اسکریپت» (scriptSig) به فیلد «شاهد» (witness) است. فیلد «کلید عمومی اسکریپت» (scriptPubKey) تراکُنش‌های P2WSH نیز با P2SH متفاوت است.

کیف‌پول کاغذی

paper wallet

کیف‌پول کاغذی (در دقیق‌ترین تعریف) سندی است حاوی تمام داده‌های لازم برای ایجاد هر تعداد دلخواه کلید خصوصی بیت‌کوین؛ این کیف در واقع مجموعه‌ای است حاوی تعدادی کلید. با این حال، بسیاری از افراد از این اصطلاح (به جای اسناد فیزیکی) برای اشاره به یک انباره‌ی آفلاین بیت‌کوین استفاده می‌کنند. این تعریف دوم نیز دربرگیرنده‌ی کلیدهای کاغذی و کُدهای قابل‌وصول است.

کانال پرداخت

payment channel

[به آن کانال ریز پرداخت نیز گفته می‌شود.] مجموعه‌ی تکنیک‌هایی که به کاربران اجازه می‌دهد تراکُنش‌های متعدد بیت‌کوین انجام دهند، بدون این که آنها را به بلاک‌چین بیت‌کوین ارجاع دهند. در یک کانال پرداخت معمولی فقط دو تراکُنش به بلاک‌چین اضافه می‌شود، در حالی که تعداد پرداخت‌های انجام‌شده بین طرفین مبادله می‌تواند تقریباً نامحدود باشد.

استخراج ائتلافی

pooled mining

یک رویکرد استخراج که در آن چند مشتری در تولید یک بلاک همکاری کرده و سپس جایزه‌ی آن بلاک را به نسبت سهم هر یک از توان پردازشی [مورد نیاز برای تولید این بلاک] تقسیم می‌کنند.

اثبات-سهم

Proof-of-Stake

روشی که یک شبکه‌ی بلاک‌چین ارز رمزبنیان برای دستیابی به اجماع توزیع‌شده به کار می‌گیرد. در روش اثبات-سهم (PoS) از کاربران خواسته می‌شود تا مالکیت خود را بر یک مقدار معین ارز («سهم» آنها در این ارز) ثابت کنند.

اثبات-کار

Proof-of-Work (PoW)

یک قطعه‌ی داده که یافتن آن به توان پردازشی زیادی نیاز داشته باشد. در بیت‌کوین، معدنچی‌ها باید جواب عددی یک الگوریتم SHA256 را بیابند که توان پردازشی مورد نیاز برای یافتن آن متناسب با معیار انتخاب‌شده توسط کل شبکه (موسوم به هدف دشواری) است.

جایزه

reward

مقدار پاداش هر بلاک جدید که توسط شبکه به معدنچی یابنده‌ی جواب PoW تخصیص داده می‌شود. در حال حاضر، مقدار این جایزه ۱۲٫۵ BTC به ازای هر بلاک است.

تابع RIPEMD-160

RIPEMD-160

یک تابع دَرهم‌سازی رمزنگاری ۱۶۰-بیتی. تابع RIPEMD-160 ویرایش تقویت‌شده‌ی تابع RIPEMD با یک خروجی دَرهم ۱۶۰-بیتی است، و انتظار می‌رود حداقل تا ۱۰ سال آینده (یا بیشتر) اَمن باشد.

ساتوشی

satoshi

کوچکترین واحد خُرد بیت‌کوین که می‌تواند در یک بلاک‌چین ثبت شود؛ این واحد که به افتخار ساتوشی ناکاموتو (خالق بیت‌کوین) نام‌گذاری شده، معادل ۰٫۰۰۰۰۰۰۰۱ [یک صدمیلیونیم] بیت‌کوین است.

ساتوشی ناکاموتو

Satoshi Nakamoto

نام فرد یا گروهی که بیت‌کوین را طراحی کرده و اولین مرجع پیاده‌سازی آن، موسوم به هسته‌ی بیت‌کوین، را ایجاد کرد. ناکاموتو (به عنوان بخشی از پیاده‌سازی بیت‌کوین) همچنین اولین پایگاه داده‌ی بلاک‌چین را طراحی کرد. اولین مسأله‌ای که در این راه باید حل می‌شد، مشکل «خرج (مصرف) دوباره» پول دیجیتال بود. هویت واقعی این فرد (یا افراد) همچنان ناشناس باقی مانده است.

«اسکریپت»

Script

در بیت‌کوین برای انجام تراکُنش از یک سیستم اسکریپت‌نویسی استفاده می‌شود. سیستم اسکریپت‌نویسی بیت‌کوین [که Script نام دارد] ساختاری شبیه زبان برنامه‌نویسی فورت (Forth) دارد. زبان Script ساده و پشته-محور است، و از چپ به راست پردازش می‌شود. این زبان اسکریپت‌نویسی عمداً طوری طراحی شده که «تورینگ-کامل» نباشد، و در آن حلقه وجود ندارد.

کلید عمومی اسکریپت (یا اسکریپت کلید عمومی)

scriptPubKey (= pubkey script)

یک اسکریپت که در خروجی گنجانده می‌شود و شرایط لازم برای خرج کردن ساتوشی‌های آن خروجی را تعیین می‌کند. داده‌های مورد نیاز برای اجرای این شرایط را می‌توان در یک اسکریپت امضا ارائه کرد.

امضای اسکریپت (یا اسکریپت امضا)

scriptSig (= signature script)

داده‌ی تولیدشده توسط خرج‌کننده (مصرف‌کننده) که تقریباً همیشه به عنوان متغیرهایی برای جواب دادن به یک اسکریپت کلید عمومی به کار می‌روند.

کلید سرّی (یا کلید خصوصی)
secret key (= private key)

عدد سرّی که برای باز کردن قفل بیت‌کوین به آدرس متناظر فرستاده می‌شود. یک کلید خصوصی چیزی شبیه 5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh است.

شاهد تفکیک‌شده
Segregated Witness

پیشنهادی برای ارتقای پروتکل بیت‌کوین که بنا بر آن داده‌ی امضا به کمک نوآوری‌های فناوری از تراکُنش بیت‌کوین جدا می‌شود. شاهد تفکیک‌شده یک انشعاب نرم محسوب می‌شود، و تغییری است که قواعد پروتکل بیت‌کوین را از نظر فنی محدودتر می‌کند.

الگوریتم *SHA*
SHA

الگوریتم دَرهم اَمن (Secure Hash Algorithm) خانواده‌ای از توابع دَرهم رمزنگاری است که توسط مؤسسه‌ی ملی استانداردها و فناوری ایالات متحده (NIST) منتشر شده است.

اعتبارسنجی پرداخت ساده
simplified payment verification (SPV)

روشی برای اعتبارسنجی تراکُنش‌های معینی از یک بلاک بدون بارگیری کل آن بلاک. روش SPV در برخی مشتری‌های سبک‌وزن بیت‌کوین به کار گرفته شده است.

انشعاب نرم
soft fork

[به آن «تغییر انشعاب‌زنی-نرم» نیز گفته می‌شود.] یک انشعاب موقتی در بلاک‌چین که معمولاً زمانی رُخ می‌دهد که معدنچی‌ها از گره‌های قدیمی (گره‌های ارتقانیافته‌ای که از قواعد جدید اجماع خبر ندارند) برای استخراج بیت‌کوین استفاده کنند. نباید آن را با «انشعاب»، «انشعاب سخت‌افزاری»، «انشعاب نرم‌افزاری» یا «انشعاب گیت» اشتباه گرفت.

بلاک کهنه
stale block

بلاک‌هایی که با موفقیت استخراج شده‌اند ولی در بهترین بلاک‌چین قرار نگرفته‌اند، احتمالاً به این خاطر که بلاک دیگری با همان ارتفاع زودتر زنجیره‌ی خود را توسعه داده است.

قفل‌زمانی
timelock

نوعی محدودیت (قید) که تا زمانی مشخص در آینده یا رسیدن به ارتفاعی معین جلوی خرج کردن (مصرف) بیت‌کوین را می‌گیرد. قفل‌زمانی نقش مهمی در بسیاری از قراردادهای بیت‌کوین دارند، از جمله در کانال‌های پرداخت و قراردادهای قفل‌زمانی دَرهم.

تراکُنش
transaction

به زبان ساده، تراکُنش یعنی انتقال بیت‌کوین از یک آدرس به آدرس دیگر. به بیان دقیق‌تر، تراکُنش یک ساختمان داده‌ی امضاشده است که یک انتقال وجه را توصیف می‌کند. تراکُنش‌ها روی شبکه‌ی بیت‌کوین ارسال می‌شوند، معدنچی‌ها آنها را تحصیل (دریافت) می‌کنند، و بعد از اضافه شدن به بلاک‌های یک بلاک‌چین، به بخشی دائمی از آن بلاک‌چین تبدیل می‌شوند.

مخزن تراکُنش *transaction pool*

یک مجموعه‌ی نامنظم از تراکُنش‌ها که در هیچ یک از بلاک‌های بلاک‌چین اصلی نیستند، ولی برای آنها تراکُنش ورودی وجود دارد.

کاملیت تورینگ *Turing completeness*

یک زبان برنامه‌نویسی را «تورینگ-کامل» می‌گویند اگر بتواند هر برنامه‌ای را که یک ماشین تورینگ قادر به اجرای آن با حافظه‌ی کافی و در زمان کافی است، اجرا کند.

خروجی تراکُنش خرج‌نشده *unspent transaction output (UTXO)*

یک خروجی تراکُنش مصرف‌نشده که می‌توان آن را به عنوان ورودی در یک تراکُنش جدید خرج کرد.

کیف‌پول *wallet*

نرم‌افزاری که تمامی بیت‌کوین‌ها و کلیدهای سرّی فرد را در خود نگه می‌دارد. از کیف‌پول می‌توان برای ارسال، دریافت، و ذخیره کردن بیت‌کوین استفاده کرد.

فرمت واردات کیف‌پول *Wallet Import Format (WIF)*

فرمت تبادل داده که برای واردات/صادرات یک کلید خصوصی واحد (به همراه پرچمی که نشان می‌دهد آیا این کلید خصوصی از یک کلید عمومی فشرده استفاده می‌کند یا خیر) طراحی شده است.

برای اطلاعات بیشتر درباره‌ی این واژه‌ها (و همچنین دیدن واژه‌های بیشتر) می‌توانید به بیت‌کوین-ویکی به آدرس https://en.bitcoin.it/wiki/Main_Page (یا سایر مستندات منبع باز آن) مراجعه کنید.