ویکی‌پدیا
دانشنامهٔ آزاد
# شبکه بیت‌کوین

از ویکی‌پدیا، دانشنامهٔ آزاد

**شبکه بیتکوین** شبکه‌ای همتابه‌همتا است که طبق پروتکلی رمزی عمل می‌کند. کاربران و بیتکوین ها (واحدهای ارز) پیام‌های امضا شده دیجیتالی را با استفاده از نرم‌افزار کیف پول بیتکوین پخش عمومی می‌کنند. تراکنش‌ها در یک پایگاه داده توزیع شده و تکثیر شده ثبت می‌گردند که زنجیره بلوکی نام دارد و از طریق سامانه اثبات عملی که معدن کاوی نامیده می‌شود در مورد مقادیر پایگاه داده توزیع شده تفاهم به وجود می‌آید. پروتکل در سال ۲۰۰۸ طراحی شد و در سال ۲۰۰۹ به عنوان یک نرم‌افزار متن باز توسط ساتوشی ناکاموتو منتشر شد.

شبکه برای اشتراک تراکنش‌ها به ساختاری حداقلی نیاز دارد. پیام‌ها طبق بهترین تلاش پخش عمومی می‌شوند و گره‌ها می‌توانند به اختیار خود شبکه را رها کرده و دوباره به آن ملحق گردند. در لحظه باز اتصال گره بلوک‌های جدید را از دیگر گره‌ها بارگیری می‌کند تا نسخه خودش از زنجیره بلوکی را کامل کند[۱][۲]

شبکه برای به اشتراک گذاری تراکنش ها به یک ساختار حداقلی نیاز دارد. برای این منظور یک شبکه غیرمتمرکز از داوطلبان میتواند کافی باشد که به آنها گره های شبکه میگویند. این گره ها (به انگلیسی: Node)میتوانند هر زمان که خواستند از شبکه جدا شوند و در صورت تمایل به بازگشت به شبکه باید بلوک های جدیدی که در زمان غیبت آنها تشکیل شده از سایر گره ها دریافت کنند و آن را به صورت لوکال در سیستم خود ذخیره کنند. این کار به منظور هماهنگی و آپدیت بودن همه گره ها ضروری است.

## محتویات



## تراکنش ها

بیت کوین در حقیقت متشکل از توالی امضا های دیجیتال است که از زمان ایجاد اولین بلوک زنجیره شبکه به عنوان پاداش پدیدآورنده آن ایجاد شده است. مالک یک بیت کوین میتواند با یک امضای دیجیتالی مالکیت آن را به شخص دیگری بدهد و به این صورت است که یک تراکنش بیت کوین صورت میگیرد. در این مرحله گیرنده می تواند با بررسی تمام تراکنش های قبلی صحت سالم بودن زنجیره و مالکیت فرستنده را اعتبار دهد. در تراکنش های بیت کوین برخلاف سیستم های سنتی، تراکنش ها بازگشت ناپذیر (به انگلیسی: irreversible) هستند و این ویژگی باعث می شود تا از حملاتی مانند دوبار خرج کردن (به انگلیسی: Double Spending) جلوگیری شود. در شبکه بیت کوین این امکان وجود دارد که هر شخص ۱ بیت کوین داشته باشد اما از آنجاییکه ممکن است آن ۱ بیت کوین مجموعی از مقادیر کمتر از ۱ بیت کوین بودند که در حال حاضر به یک دارنده تعلق دارد؛ هر تراکنش شامل تراکنش های در دل خود می شود که میتواند ورودی ها و خروجی های زیادی داشته باشد. در حالت کلی معمولا یک تراکنش شامل یک ورودی است که تراکنش قبلی را شامل می شود یا متشکل از ورودی های خرد و کوچک تری است که مجموع آنها مقدار هدف را تشکیل

میدهد. در مقابل خروجی نیز معمولا یک یا دو مورد است: مقداری که فرستنده قصد دارد آن را ارسال کند و مقداری اضافی که باید به حساب او بازگردد.

# ماینینگ

استخراج بیت‌کوین (به انگلیسی: Bitcoin Mining) اصطلاحاً به فرآیندی گفته می‌شود که طی آن با استفاده از سخت‌افزارهای ویژهٔ رایانه‌ای در شبکه بیتکوین، قادر به حل مسائل رمزنگاری، تأیید صحت یک تراکنش و نهایتاً ایجاد یک بلوک در زنجیره بلوکی (بلاک چین) بیت‌کوین شد. افرادی که مجهز به این سخت‌افزارها در شبکهٔ بیت‌کوین هستند، با تأیید تراکنش و تولید بلوک، مقداری بیت‌کوین (بنا به میزان سختی شبکه در لحظه) به عنوان پاداش دریافت خواهند کرد. این میزان در سال ۲۰۱۷ میلادی ۱۲٫۵ بیت‌کوین بود.

به زبان ساده می‌توان گفت برای این که تراکنش های بیت کوین یا هر ارز دیگر و همین طور امنیت آن فرایند ماینینگ صورت پذیرد این دستگاه های ماینینگ امنیت ارز دیجیتال بیت کوین را تامین می‌کنند و برای همین شبکه بیت کوین یک جایزه برای دلگرمی و تشویق صاحبان ماینینگ به آنها می‌دهد که یک مقدار بیت کوین به میزان تلاش آن ماینر خواهد بود. این فرایند تقریباً در تمام ارزها یکسان است. پیش بینی می‌شود در سال ۲۰۲۴ تعداد پاداش برای ماینرها نصف شود یعنی ۶/۲۵.

## تاریخچه

از زمانی که بیت‌کوین توسط خالق آن، ساتوشی ناکاموتو، خلق شد تا به امروز دچار تغییراتی شده که در اوراق سفید ساتوشی از همان ابتدا به آن اشاره شده بود. میزان استخراج و توان استخراج‌کنندگان در شبکه به میزان سختی شبکهٔ بیت‌کوین بستگی دارد. در سال ۲۰۰۹ که نخستین بلوک‌های زنجیرهٔ بلوکی بیت‌کوین در حال شکل گرفتن بود، سختی شبکه بسیار کمتر از حال حاضر بود. این موضوع باعث می‌شد تا بتوان با سخت‌افزارهای ساده‌تر (حتی با رایانه‌های شخصی) بتوان بیت‌کوین تولید کرد. به همین دلیل نیز از سال ۲۰۰۹ تا ۲۰۱۷ چیزی حدود ۱۷ میلیون از کل ۲۱ میلیون بیت‌کوین موجود استخراج شد. اما رفته رفته با بالا رفتن سختی شبکه، سخت‌افزارهای خاصی با نام اسیک (ASIC) انحصاراً برای استخراج بیت‌کوین طراحی شد.[۳]

## دستگاه استخراج بیت‌کوین

با توجه به افزایش شدید سختی شبکه و تقاضای زیاد برای استخراج بیت‌کوین، سخت‌افزارهایی با نام اسیک (ASIC) تولید شده‌اند. اسیک مخفف اصطلاح مدارهای مجتمع با کاربردهای خاص می‌باشد که صرفاً برای استخراج و تولید بیت کوین طراحی شده‌اند. این اسیک‌ها انواع مختلفی دارند و با توجه میزان هش پاور یا قدرت هش که تولید می‌کنند، قیمت‌های متفاوتی دارند.

## میزان مصرف انرژی استخراج بیت‌کوین

سخت‌افزارهای استخراج معمولاً برق زیادی مصرف می‌کنند و به دلیل اینکه مدام باید به شبکه بیت‌کوین متصل باشند، نباید خاموش شوند. همین موضوع باعث افزایش دمای این دستگاه‌ها می‌شود و برای جلوگیری از سوختن دستگاه حتماً باید از فن و دستگاه‌های خنک‌کننده استفاده شود؛ بنابراین مجموعه پکیج استخراج بیت‌کوین می‌تواند انرژی زیادی را مصرف کند. این موضوع نگاه سازمان‌های محیط زیست جهانی و استفاده از انرژی پاک را به خود جلب کرده‌است.[۴]

در همین راستا تیم توسعه‌دهندهٔ بیت‌کوین و جامعهٔ فعال این ارز رمزنگاری‌شده تلاش می‌کنند تا راه‌های حل این مشکل را پیاده‌سازی کنند.

## استخراج بیت کوین با گوشی یا رایانهٔ شخصی

گوشی همراه یا رایانه شما هر چقدر هم که پیشرفته باشد، با به‌کارگیری آن برای استخراج بیت‌کوین خیلی زود مستهلک خواهد شد. سخت‌افزارهایی که در گوشی و رایانه شما تعبیه شده‌اند نیاز به باتری یا برق دارند و بهتر است بگوییم با انجام این کار نخستین قسمتی که نابود خواهد شد، باتری دستگاه شما است.[۵]

# منابع


۱. Nakamoto, Satoshi (24 May 2009). "Bitcoin: A Peer-to-Peer Electronic Cash System" (https://bitcoin.org/bitcoin.pdf) (PDF). Retrieved 20 December 2012.

۲. Barber, Simon; Boyen, Xavier; Shi, Elaine & Uzun, Ersin (2012). "Bitter to Better — how to make Bitcoin a better currency" (http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf) (PDF). *Financial Cryptography and Data Security*. Springer Publishing.

۳. PeopleVine, Sigenics via. "What is an ASIC, and why is everyone using them? - Sigenics" (http://www.sigenics.com/blog/what-is-an-asic). Retrieved 2018-10-07.

۴. Reiff، Nathan (۲۰۱۸-۰۳-۰۸). «How Much Does It Cost to Mine Bitcoin Around the World?» (https://www.investopedia.com/news/how-much-does-it-cost-mine-bitcoin-around-world/) (به انگلیسی). Investopedia. دریافت‌شده در ۲۰۱۸-۱۰-۰۷.

۵. «استخراج بیت کوین با گوشی و کامپیوتر به صرفه نیست! - میهن بلاکچین» (https://mihanblockchain.com/blog/articles/mining-computer-mobilephone/). میهن بلاکچین. ۱۳۹۷-۰۶-۲۶T22:17:29+00:00. دریافت‌شده در 2018-11-03. تاریخ وارد شده در |تاریخ= را بررسی کنید (کمک)