راهنمای بیت‌کوین

نگاهی به شیوه‌های دریافت، سرمایه‌گذاری و
پرداخت اولین ارز رمزنگاری شده غیرمتمرکز جهان

یان دی‌مارتینو

احمدمیردامادی
رضاقربانی‌وپیمان‌رحمانی

راه‌پرداخت

altcoin
معادل فارسی آن، آلت‌کوین است و مخفف عبارت «Alternative Cryptocurrency» به معنای «رمزارز جایگزین» است. آلت‌کوین، رمزارز دیگری مشابه با بیت‌کوین است. در حال حاضر، بیش از هزار آلت‌کوین وجود دارند. اکثر آنها، رونوشت (کپی)های کاملا دقیق ارزهای رمزنگاری شده موفق‌تر به‌شمار می‌روند، اما برخی از آنها نیز ایده‌های کاملا جدیدی محسوب می‌شوند.

ASIC
مخفف عبارت «Application-Specific Integrated Circuit» به معنای «مدار مجتمع با کاربرد خاص» است. ASIC، به قطعه سخت‌افزاری‌ای اشاره دارد که تنها و تنها برای انجام یک کار، طراحی شده است. در دنیای رمزارزها، ASIC، به یک الگوریتم خاص، مثل SHA۲۵۶ و Scrypt، اشاره می‌کند.

BFGMiner
دومین نرم‌افزار محبوب استخراج بیت‌کوین است.

Bitcoin/bitcoin
معادل فارسی آن، بیت‌کوین است. Bitcoin با حرف بزرگ انگلیسی، به سیستم، شبکه یا ارز بیت‌کوین، به مفهوم کلی آن اشاره می‌کند، اما bitcoin با حرف کوچک انگلیسی، به بیت‌کوین‌های مجزا اشاره دارد، مثل اینکه بگوییم «من پنج بیت‌کوین دارم.»

Bitcoin-Qt
نام دیگر آن هسته بیت‌کوین (Bitcoin core) است که به پیاده‌سازی اولیه بیت‌کوین اشاره دارد و پایه و اساس همه کیف پول‌ها و سرویس‌ها را تشکیل می‌دهد.

Bitcoin XT
پیاده‌سازی جایگزینی برای هسته بیت‌کوین است که با پیاده‌سازی اصلی فعلی بیت‌کوین سازگار است و ابتدا توسط گوین آندرسن و مایک هیرن مطرح شد. از این نرم‌افزار، برای تست ویژگی‌های جدید استفاده می‌شود و دلیل مطرح شدن آن به عدم توافق بر سر اندازه بلوک در Bitcoin-Qt برمی‌گشت. اپلیکیشن فوق‌الذکر، بلوک‌های با اندازه ۲۰ مگابایت را به‌عنوان یک ویژگی اولیه، معرفی کرد.

block
معادل فارسی آن بلوک است. تراکنش‌های موجود در بلاکچین، به بلوک‌های مختلفی تقسیم می‌شوند و این بلوک‌ها، تقریبا هر ۱۰ دقیقه، توسط استخراج‌گرها، تایید می‌شوند.

blockchain
معادل فارسی آن، بلاکچین است. بلاکچین، دفتر کلی غیرمتمرکز به‌شمار می‌رود که مبنای کار بیت‌کوین است. هر تراکنش و حساب، از طریق این دفتر کل، ردیابی خواهد شد. این نام را با نام وبگاه .Blockchain info یا شرکت Blockchain، اشتباه نگیرید. این عبارت، به هر فناوری جدیدی که از یک دفتر کل برای ردیابی ارزش دیجیتال استفاده می‌کند نیز اشاره دارد.

block explorer
معادل فارسی آن، کاوشگر بلوک است. کاوشگر بلوک، به یک وبگاه یا قطعه نرم‌افزاری اشاره دارد که امکان مشاهده و دنبال کردن تراکنش‌های بیت‌کوین را از طریق زنجیره بلوک، فراهم خواهد ساخت. علاوه بر این، می‌توان از آن، جهت توصیف سیستم‌های مشابه موجود در بلاکچین‌های آلت‌کوین‌ها نیز استفاده کرد.

CGMiner
محبوب‌ترین نرم‌افزار استخراج بیت‌کوین است.

cold wallet
معادل فارسی آن، کیف پول برون‌خط (آفلاین) یا سرد است. کیف پول سرد، به کیف پولی روی یک رایانه یا دیسک ذخیره‌ساز اطلاق می‌شود که به اینترنت متصل نیست. این نوع کیف پول، باید برای تایید تراکنش‌ها، به اینترنت متصل شده و به یک کیف پول برخط تبدیل شود. بعد از تایید و امضای تراکنش، کیف پول برخط، می‌تواند مجددا به کیف پول برون‌خط تبدیل شود.

core developer
معادل فارسی آن، توسعه‌دهنده هسته است. توسعه‌دهنده هسته، به فرد توسعه‌دهنده یک رمزارز می‌گویند که به دستورات git commit واقع در صفحه پلتفرم توسعه سایت GitHub دسترسی دارد.

cryptocurrency
معادل فارسی آن، رمزارز است. به هر ارز دیجیتال که برای تامین امنیت سیستمش یا هویت کاربران و نگهدارندگان حساب، از فناوری رمزنگاری (cryptography) بهره می‌گیرد، رمزارز می‌گویند.

Dark web
معادل فارسی آن، وب تاریک است. به بخشی از وب عمیق که از سرویس‌های خاصی ساخته می‌شود، وب تاریک می‌گویند. مثلا فعالیت‌های حوزه مواد مخدر، در چنین محیطی انجام می‌شوند. به‌طور کلی، هر فعالیتی از قبیل روزنامه‌نگاری که ممکن است مستلزم ناشناس ماندن افراد باشد، در محیط وب تاریک، قابل انجام خواهد بود.

Decentralization
معادل فارسی آن، غیرمتمرکزسازی است. مطابق این ایده، مالکیت یک شبکه، سرویس یا شرکت را می‌توان بین گروه بزرگی از افراد، توزیع کرد، به نحوی که هیچ نقطه شکست متمرکزی وجود نداشته باشد. مثلا، اینترنت، یک شبکه ارتباطی سراسری و غیرمتمرکز به‌شمار می‌رود.

Deep Web
معادل فارسی آن، وب عمیق یا وب پنهان است. به همه داده‌های موجود در اینترنت که توسط مرورگرهای وب معمولی قابل مشاهده نیستند، از اطلاعات بانکداری گرفته تا بازارهای غیرقانونی مواد مخدر، وب عمیق می‌گویند.

ecash/emoney
معادل فارسی آن، پول (money) الکترونیکی است. پول الکترونیکی، به هر نوعی از پول دیجیتال اطلاق می‌شود که از دنیای واقعی فاصله دارد. معمولا به ارزهای دیجیتال قبل از بیت‌کوین، پول الکترونیکی می‌گویند.

faucet
فاست‌ها، سرویس‌هایی روی وب هستند که برای انجام وظایف کوچکی از قبیل مشاهده تبلیغات، بخش کمی از بیت‌کوین را به‌صورت مجانی در اختیار کاربران قرار می‌دهند. به بیان دیگر، به فاست‌ها، سرویس‌های کسب درآمد قطره‌ای بیت‌کوین می‌گویند. وقتی بیت‌کوین ارزش چندان بالایی نداشت، فاست‌ها، بیت‌کوین‌های کامل را نیز در اختیار کاربران قرار می‌دادند. اما امروزه، حتی بخش بسیار کوچکی از یک بیت‌کوین هم، درست به اندازه همان بیت‌کوین‌های کامل قبلی، با بخش‌های کوچکی از یک سنت، برابری می‌کنند.

attack 51%

معادل فارسی آن، حمله ۵۱ درصدی است. بیت‌کوین، برای اعتبارسنجی زنجیره بلوک، از سیستمی به نام «سند کار» (proof of work) بهره می‌گیرد. سند کار، برای اعتبارسنجی و تایید تراکنش‌ها، به توان محاسباتی بالایی نیاز دارد. تغییر یک تراکنش، داده‌های قابل تایید موجود در همه تراکنش‌های بعدی را تغییر خواهد داد. بنابراین، اگر دو بلاکچین رقیب، با تاریخچه‌های تراکنش مختلف وجود داشته باشند، بلاکچین طولانی‌تر، به‌عنوان بلاکچین غیرکاذب یا true در نظر گرفته خواهد شد، زیرا بیشترین توان محاسباتی را در اختیار دارد. از آنجایی که بازیگران خرابکار، معمولا به‌تنهایی کار می‌کنند، بعید است که هیچ گروه منفردی بتواند در قیاس با بلاکچین حقیقی، توان محاسباتی بیشتری را برای بلاکچین اصلاح‌شده‌اش، در اختیار بگیرد. با این حال، اگر گروهی بتواند نرخ هَش بیشتری را نسبت به نرخ هش ترکیبی همه استخراج‌گرهای در حال کار روی بلاکچین، در دست بگیرد، آنگاه موفق‌تر از زنجیره معتبر عمل خواهد کرد و تایید اعتبار بلاکچین خودش را دریافت خواهد کرد. به این اتفاق، حمله ۵۱ درصدی می‌گویند.

fork

معادل فارسی آن، انشعاب است. به رونوشت (کپی) کردن یک کد منبع‌باز و تغییر دادن آن، انشعاب می‌گویند. در حوزه رمزارزها، زمانی که استخراج‌گرها، به‌صورت تصادفی یا به‌منظور خرابکاری، به استخراج یک زنجیره بلوک غیرکاذب دست می‌زنند نیز، فرایند انشعاب اتفاق می‌افتد.

full node

معادل فارسی آن، گره کامل است. یک کیف پول بیت‌کوین محلی که کل بلاکچین را ذخیره می‌سازد و به اعتبارسنجی و گسترش تراکنش‌های تاییدشده از طریق استخراج‌گرها، کمک می‌کند. بر خلاف استخراج‌گرها، گره‌های کامل، به هیچ سخت‌افزار اختصاصی‌ای نیاز ندارند و هیچ پاداشی را نیز دریافت نمی‌کنند.

git commit

به هر تغییر ممکن در کد منبع‌باز واقع در وبگاه GitHub، اطلاق می‌شود.

GitHub

وبگاهی است که کدهای منبع‌باز را جهت کار مشترک روی آنها، میزبانی می‌کند.

GUIMiner

محبوب‌ترین نرم‌افزار استخراج بیت‌کوین بوده که دارای رابط کاربر گرافیکی است.

hard fork

معادل فارسی آن، انشعاب سخت است. به آن دسته از تغییرات صورت‌گرفته در کد رمزارز که پس از انجام آنها، کاربران باید جهت ادامه کار با کلاینت‌های ارتقایافته، نرم‌افزارشان را ارتقا بدهند، انشعاب سخت می‌گوییم. اگر بخش عمده کاربران، ارتقای نرم‌افزاری را انجام ندهند، نرم‌افزار قدیمی‌تر، همچنان عمل استخراج را روی بلاکچین‌اش ادامه خواهد داد. از آنجایی که این بلاکچین، طولانی‌تر خواهد بود و از نرخ هش بیشتری بهره خواهد گرفت، در نتیجه، شبکه کوین، به دو قسمت تقسیم می‌شود که احتمال بروز فاجعه را بالا خواهد برد. با این حال، انشعاب‌های سخت موفق، در اغلب اوقات، تنها شیوه برای انجام تغییرات قابل توجه در کد رمزارز به‌شمار می‌روند.

hash

معادل فارسی آن، هَش یا درهم‌سازی است. هش، یک واحد اندازه‌گیری محسوب می‌شود که میزان توان محاسباتی ارائه‌شده در شبکه را نشان خواهد داد.

hashing power
معادل فارسی آن، توان هشینگ یا توان درهم‌سازی است، عبارت انگلیسی دیگری برای hashrate است.

hashrate
معادل فارسی آن، نرخ هَش یا نرخ درهم‌سازی است. به تعداد کل هش‌های ارائه‌شده در یک شبکه، نرخ هش می‌گویند. تعداد کل هش‌ها، برابر با تعداد معادلات محاسباتی انجام‌گرفته در شبکه بیت‌کوین (یا سایر رمزارزها) است. منظور از نرخ هش ۱THs/، آن است که شبکه می‌تواند یک تریلیون محاسبه را در هر ثانیه انجام بدهد.

hot wallet
معادل فارسی آن، کیف پول برخط (آنلاین) یا گرم است. به کیف پول متصل به اینترنت، کیف پول برخط می‌گویند. در صورتی که رایانه یا گذرواژه مربوط به کیف پول، فاقد امنیت باشد، احتمال خطر دزدیده شدن بیت‌کوین‌ها وجود خواهد داشت. کیف پول برخط، برای ذخیره‌سازی کوتاه‌مدت و خرج کردن پول، مناسب است. همه کیف پول‌های وب، کیف پول‌های برخط هستند.

lead developer
معادل فارسی آن، توسعه‌دهنده پیشرو است. توسعه‌دهنده پیشرو، تعیین می‌کند که کدام توسعه‌دهندگان می‌توانند به دستورات git commit، دسترسی داشته باشند.

local wallet
معادل فارسی آن، کیف پول محلی است. هر یک از کیف پول‌های برون‌خط یا برخط که روی رایانه شما ذخیره شده‌اند، کیف پول محلی به‌شمار می‌روند.

miner
معادل فارسی آن، استخراج‌گر یا ماینر است. به هر شرکت‌کننده در شبکه بیت‌کوین که محاسبات ریاضی پیچیده‌ای را برای تامین امنیت شبکه بیت‌کوین انجام می‌دهد و علاوه بر آن، هر تراکنش صورت‌گرفته از طریق رمزنگاری را تایید می‌کند، استخراج‌گر می‌گویند. همچنین، به سخت‌افزار کامپیوتری واقعی‌ای که این کار را انجام می‌دهد و همچنین افراد یا شرکت‌هایی که مالک این سخت‌افزار هستند استخراج‌گر می‌گوییم.

mining
معادل فارسی آن، استخراج است. به فرایند تایید تراکنش‌های بیت‌کوین، در قالب گروه‌هایی به نام بلوک، از طریق حل کردن محاسبات ریاضی پیچیده و سپس ارسال این تراکنش‌ها به بقیه بخش‌های شبکه، استخراج گفته می‌شود. برای انجام این کار، استخراج‌گرها، بخش کمی از بیت‌کوین را به‌عنوان جایزه دریافت می‌کنند که نحوه ایجاد بیت‌کوین‌های جدید را نشان خواهد داد. علاوه بر این، استخراج‌گرها، کارمزدهای کوچکی را نیز که به هر تراکنش پیوست شده است، دریافت خواهند کرد که با توجه به تعداد ۲۱ میلیون بیت‌کوین استخراج‌شده کنونی، برآورد می‌شود که تعداد آنها در سال به ۲۱۴۰ عدد برسد. استخراج‌گرها، همواره در حال رقابت با یکدیگر هستند.

Mt.Gox
معادل فارسی آن، مت گاکس است. مت گاکس، وبگاه برخطی است که هدف اولیه آن به خریدوفروش کارت‌های Magic The Gathering Card برمی‌گشت، اما در نهایت، به اولین و بزرگ‌ترین مرکز مبادلات بیت‌کوین و اولین بازار آزاد متمرکز در این حوزه تبدیل شد. شرکت مت گاکس، بعد از خرابی‌های امنیتی مختلف و متهم شدن به کلاهبرداری، در اوایل سال ۲۰۱۴، اعلام ورشکستگی کرد.

node runner

معادل فارسی آن، اداره‌کننده گره است. اداره‌کننده گره، شرکت‌کننده‌ای در شبکه بیت‌کوین است که کل بلاکچین را دانلود می‌کند و کار استخراج‌گر را مورد بررسی مضاعف قرار می‌دهد، اما در رقابت جهت استخراج بیت‌کوین شرکت ندارد و هیچ جایزه‌ای را دریافت نمی‌کند، ولی با این وجود، بخش مهمی در فرایند تامین امنیت شبکه بیت‌کوین به‌شمار می‌رود. با بزرگ‌تر شدن اندازه زنجیره‌های بلوکی و کاهش تعداد افرادی که می‌خواهند کل یک چیز را دانلود کنند، بحث افزایش مشوق‌ها برای اداره‌کننده‌های گره، مورد توجه بیشتری قرار گرفته است.

open-source

معادل فارسی آن، منبع‌باز یا اوپن‌سورس است. به کدی که باز باشد و هر کسی بتواند آن را تغییر بدهد، منبع‌باز می‌گویند.

paper wallet

معادل فارسی آن، کیف پول کاغذی است. به کلید خصوصی یا عمومی که روی یک تکه کاغذ، نوشته یا چاپ می‌شود، کیف پول کاغذی می‌گوییم.

pre-mine

معادل فارسی آن، پیش‌استخراج است. وقتی آلت‌کوین‌ها برای اولین بار ایجاد می‌شوند، سازندگان آنها گاهی اوقات قبل از فعال شدن شبکه، تعدادی کوین را تولید می‌کنند و افراد مختلف می‌توانند به شیوه‌ای منصفانه، آنها را استخراج کنند. به‌طور کلی، پیش‌استخراج، نشانه اسکم (کلاهبرداری) است، اما اگر تعداد کوین‌ها پایین باشد و این کار با شفافیت بالایی صورت بگیرد، در آن صورت، برنامه کوین، فاقد اسکم خواهد بود.

proof-of-burn (PoB)

معادل فارسی آن، سند حیف و میل است. به استفاده از بلاکچین، برای اثبات این موضوع که بیت‌کوین یا رمزارز دیگری دارد به یک آدرس غیرقابل مصرف می‌رود و برداشتن موثر آن در سیستم، سند حیف و میل می‌گویند.

proof-of-stake (PoS)

معادل فارسی آن، اثبات سهام است. سند سهام، نوعی اثبات رمزنگاری به‌شمار می‌رود که امنیت بلاکچینی را که رای‌ها را بر اساس توان محاسباتی اندازه‌گیری می‌کند، تضمین خواهد کرد.

public-key encryption

معادل فارسی آن، رمزگذاری کلید عمومی است. در این شیوه، هر فرد غیرخودی، می‌تواند اطلاعات را بدون افشای آن، از طریق یک کلید قابل شناسایی عمومی، تایید کند. با استفاده از کلید فوق‌الذکر، می‌توان مشخص کرد که آیا یک پیغام، از جانب فردی که کلید خصوصی مرتبط با آن را در اختیار دارد، برای شما آمده است یا خیر. در این فرایند، نیازی به افشای جزئیات مربوط به آن کلید خصوصی نیست.

Scrypt

الگوریتم رایانه‌ای استفاده‌شده توسط لایت‌کوین (litecoin) و بسیاری از رمزارزها جایگزین دیگر، جهت تامین امنیت شبکه مربوط به آنها. این الگوریتم، مقاومت بیشتری نسبت به ASICها دارد.

SHA256
الگوریتم رایانه‌ای استفاده‌شده توسط بیت‌کوین و بسیاری از رمزارزهای دیگر، جهت تامین امنیت شبکه مربوط به آنها.

sidechain
معادل فارسی آن، زنجیره جانبی است. زنجیره جانبی، راهکاری برای تغییر مقیاس بیت‌کوین به‌شمار می‌رود. به عبارت دیگر، زنجیره‌های جانبی، دفاتر کل شبه بلاکچین هستند که تعداد زیادی از تراکنش‌های اضافه‌شده به بلاکچین نهایی را به‌صورت فشرده، ردیابی خواهند کرد.

soft fork
معادل فارسی آن، انشعاب نرم است. در انشعاب نرم، کد رمزارز، تغییر قابل توجهی پیدا می‌کند و با وجود اینکه ممکن است به دلایل امنیتی یا دلایل دیگر، به ارتقای نرم‌افزار کیف پول نیاز داشته باشیم، اما نرم‌افزار قدیمی‌تر، همچنان می‌تواند تراکنش‌ها را ارسال، دریافت و اعتبارسنجی کند و امکان اعتبارسنجی اتفاقی و تصادفی بلاکچین‌های دیگر وجود نخواهد داشت.

wallet
معادل فارسی آن، کیف پول است. این عبارت کلی، به نرم‌افزاری اشاره دارد که جهت تایید و امضای تراکنش‌های صورت‌گرفته با استفاده از آدرس بیت‌کوین شما، باید با شبکه بیت‌کوین ارتباط برقرار کند.

web wallet
معادل فارسی آن، کیف پول وب است. به هر کیف پولی که از طریق وبگاه نگهداری‌شده توسط شرکت دیگر، کنترل و محافظت می‌شود، کیف پول وب می‌گویند. امنیت و میزان اعتماد کیف پول وب، تنها به شرکتی بستگی دارد که آن را میزبانی کرده است. به‌طور کلی، این نوع کیف پول، فقط به درد خرج کردن پول می‌خورد، اما برخی از این سرویس‌ها، امنیت بیشتری را فراهم می‌کنند و به‌دلیل استفاده از فناوری چندامضایی (multisig) و تولید کلید برون‌خط، استفاده از آنها برای ذخیره‌سازی کوتاه‌مدت تا میان‌مدت، مانعی ندارد.

X11
الگوریتم استفاده‌شده توسط Dash و تعدادی از ارزهای دیگر است. الگوریتم مزبور، همان‌طور که از نامش پیداست، از ۱۱ الگوریتم مختلف بهره می‌گیرد.