

فرهنگ توصیفی اصطلاحات بیت کوین

نسخه اول

وبسایت منابع فارسی بیت کوین

سخنی با خوانندگان

درک بیت کوین برای افرادی که به تازگی با آن آشنا شده‌اند بسیار دشوار است. به این دلیل که پیش‌نیاز درک بیت کوین، کسب دانش پایه‌ای در حوزه‌های متعددی است که لزوماً ارتباطی با یکدیگر ندارند. بیت کوین محل تلاقی علوم ریاضی، علوم کامپیوتر، اقتصاد، رمزنگاری، حریم خصوصی، و دیگر علوم است و یادگیری مطالب لازم در این حوزه‌ها به صرف زمان و مطالعه زیادی نیاز دارد.

ما در سایت منابع فارسی بر این باوریم که در دسترس بودن یک فرهنگ که اصطلاحات بیت کوین در آن به زبانی ساده توصیف شده باشند، می‌تواند کمک بزرگی در راه یادگیری و درک بیت کوین به علاقه‌مندان - خصوصاً افرادی که به تازگی به این حوزه وارد شده‌اند - باشد. تلاش می‌کنیم به مرور زمان کلمات بیشتری به این فرهنگ اضافه و آن را کامل کنیم. اگر مایل به مشارکت در گردآوری این فرهنگ هستید، از طریق ایمیل سایت با ما در ارتباط باشید.

الف. آزاد

پاییز ۱۴۰۰

تقديم به ضياء صدر

اگر یک فرد یا نهاد متقلب بخواهد تراکنشی را به نفع خود از یکی از بلاک‌های زنجیره بیت کوین حذف یا به آن اضافه کند، باید اثبات کار بلاک مورد نظر و همه بلاک‌هایی که بعد از آن ایجاد شده‌اند را دوباره از اول محاسبه کند. علاوه بر این، برای متقاعد ساختن نودهای شبکه، مبنی بر معتبر بودن بلاک‌هایی که به تازگی ایجاد شده‌اند، باید بلاک‌های جدید را سریع‌تر از همه ماینرهای حاضر در شبکه تولید کند. زیرا نودهای شبکه بیت کوین همواره طولانی‌ترین زنجیره‌ای که دارای بیشترین اثبات کار است را به عنوان زنجیره معتبر قبول می‌کنند.

یک ماینر متقلب، برای رسیدن به این هدف باید ۵۱ درصد از قدرت استخراج شبکه بیت کوین را در اختیار داشته باشد. به عبارت دیگر، توان محاسباتی او باید از مجموع توان محاسباتی سایر ماینرها بیشتر باشد. اجرای چنین حمله‌ای روی شبکه بیت کوین تقریباً ناممکن است، بنابراین شبکه بیت کوین در برابر کلاهبرداری و برگشت خوردن تراکنش‌ها مصون است. برگشت ناپذیری تراکنش‌ها بدان معنی است که بازپس‌گیری بیت کوین‌های ارسال شده - پس از تأیید - به هیچ وجه ممکن نیست.

ترس از حمله ۵۱ درصد باعث می‌شود که میزان توان هش موجود در شبکه اهمیت داشته باشد، زیرا نرخ توان هش موجود در شبکه در واقع نمایانگر کل ظرفیت استخراج شبکه بیت کوین است و هرچه این عدد بیشتر باشد، اجرای یک حمله ۵۱ درصدی گران‌تر خواهد بود. بنابراین میزان توان هش موجود در شبکه، معیاری برای سنجش امنیت شبکه در برابر حمله ۵۱ درصد است.

A

آدام بک

Adam Back

آدام بک یک متخصص علم رمزنگاری و یک سایفرپانک است. او در سال ۱۹۷۰ در شهر لندن به دنیا آمد و در حال حاضر در کشور مالتا زندگی می‌کند. او سیستم «هَش‌کَش» را برای مقابله با اسپم طراحی و پیاده‌سازی کرد و این سیستم امروزه در صنعت استخراج بیت کوین و برخی از آلت کوین‌ها مورد استفاده قرار می‌گیرد. وی از اولین افرادی است که روی بیت کوین مشغول به کار شد و در سال ۲۰۰۹ شخص ساتوشی ناکاموتو با او تماس گرفته و نظر او را در مورد استفاده از هَش‌کَش در بیت کوین جویا شده بود. او یکی از بنیان‌گذاران شرکت بلاک‌استریم است. این شرکت در گذشته یکی از مشارکت‌کنندگان اصلی در بهبود نرم‌افزار بیت کوین بوده است.

آدام بک به‌عنوان مدیرعامل شرکت بلاک‌استریم این شرکت را به یکی از توسعه‌دهندگان پیشرو در شبکه لایتنینگ، زنجیره جانبی «لیکوئید»، و دیگر پروژه‌های جالب، تبدیل کرد. مشارکت او در بیت کوین و علم رمزنگاری او را امروز به یکی از کارشناسان اصلی این حوزه تبدیل کرده است. او به‌طور فعال در مورد موضوعاتی از قبیل حریم خصوصی، مقیاس‌پذیری بیت کوین، و آینده توسعه بیت کوین سخنرانی‌هایی برگزار می‌کند.

امضای تطبیقی

Adaptor Signature

یک امضای تطبیقی امضایی است که به منظور افشای یک داده مخفی با یک امضای اولیه ترکیب می‌شود. امضای تطبیقی به دو طرف یک معامله اجازه می‌دهد بدون نیاز به اعتماد میان طرفین، دو تکه داده حساس را در زمان مناسب برای یکدیگر افشا کنند. این روش در معاملات همزمان، مانند مبادلات تهاتری کاربرد دارد.

می‌توان با یک داده محرمانه، یک امضای تطبیقی، و یک امضای معمولی یک امضای تطبیقی ایجاد

کرد. با معلوم بودن هر ۲ داده از ۳ داده این چیدمان، می توان سومی را محاسبه کرد. یک ویژگی قدرتمند امضاهای تطبیقی این است که یکی از طرفین معامله می تواند بر اساس یک داده محرمانه یک امضای تطبیقی ایجاد کند، و طرف مقابل نیز می تواند امضای تطبیقی خود را بر اساس همان داده ها تولید کند بدون اینکه نیاز باشد از داده های محرمانه طرف مقابل اطلاع داشته باشد.

به عنوان مثال، آوا و بابک قصد دارند یک بیت کوین با یکدیگر تهاتر کنند. ابتدا، آوا یک امضای تطبیقی از تراکنش امضاء نشده ای که ۱ بیت کوین به بابک ارسال می کند را به او می دهد. این تراکنش هنوز توسط آوا امضاء نشده است، بنابراین هنوز امکان منتشر شدن روی شبکه بیت کوین را ندارد، ولی به مقدار محرمانه ای که در آن وجود دارد پایبند است. در مرحله بعد، بابک تراکنشی ایجاد می کند که در آن ۱ بیت کوین به آوا ارسال می شود. بابک می تواند امضای تطبیقی خود را با استفاده از امضای تطبیقی آوا بسازد. این امضای تطبیقی به همان مقدار محرمانه پایبند است، هرچند بابک از آن اطلاع ندارد. بابک تراکنش خود و امضای تطبیقی خود را با آوا به اشتراک می گذارد.

از آنجا که آوا امضای تطبیقی و داده مخفی را در اختیار دارد، قادر است امضای تراکنش بابک را تولید کند و با ارسال تراکنش به شبکه، ۱ بیت کوین خود را مطالبه کند. بابک به محض مشاهده تراکنش امضا شده اش روی زنجیره بیت کوین، می تواند با استفاده از امضای تطبیقی و امضای اولیه خود، داده مخفی را محاسبه کند. با استفاده از این داده مخفی او می تواند امضای تراکنش آوا را بدست آورد. بابک اکنون می تواند تراکنش آوا را امضاء و او نیز ۱ بیت کوین خود را با ارسال این تراکنش به شبکه مطالبه کند.

Address

آدرس

آدرس برای دریافت بیت کوین بکار گرفته می شود و به صورت رشته ای از حروف و اعداد به نمایش در می آید. معمولاً مفهوم آدرس و کلید عمومی به جای یکدیگر بکار گرفته می شوند ولی آدرس در واقع هش یک کلید عمومی است. در حال حاضر برای دریافت بیت کوین از آدرس ها، و نه کلیدهای عمومی استفاده می شود. از نظر فنی یک آدرس علاوه بر هش کلید عمومی، اطلاعات بیشتری را در خود ذخیره می کند. کاربران می توانند توسط یک کیف پول بیت کوین به هر مقدار که نیاز داشته باشند، آدرس تولید کنند. کاربران کیف پول ها همچنین قادرند به آدرس های دیگران

بیت کوین ارسال کنند. هنگامی که بیت کوین به یک آدرس ارسال می شود، فقط صاحب کلید خصوصی ای که این آدرس از آن مشتق شده، قادر به خرج کردن یا ارسال آن برای دیگران است.

پیشنهاد می شود برای حفظ حریم خصوصی از یک آدرس دو بار برای دریافت بیت کوین استفاده نشود. هر وقت قصد دریافت بیت کوین دارید، باید از یک آدرس جدید که توسط کیف پول شما ساخته شده است استفاده کنید.

از نظر فنی، هر آدرس نماینده یک اسکرپت است و برای نشان دادن نوع اسکرپت خود کدبندی، و یک پیشوند مشخص به آن اضافه می شود. آدرس های قدیمی از روش کدبندی پیس-۵۸ استفاده می کنند و اگر هش یک کلید عمومی باشند، به آن ها آدرس های نوع P2PKH گفته می شود و با شماره «۱» شروع می شوند. آدرس های قدیمی به ندرت هش یک اسکرپت هستند و در این صورت با شماره «۳» شروع می شوند. در حال حاضر همه آدرس های نسخه صفر سگویت از روش کدبندی پیس-۳۲ استفاده می کنند و با پیشوند «bc1q» شروع می شوند.

هنگامی که یک کاربر آدرسی را در کیف پول خود وارد می کند و قصد ارسال بیت کوین به این آدرس را دارد، کیف پول نوع آدرس را بررسی و اسکرپت مورد نیاز را تولید می کند. این اسکرپت scriptPubKey نامیده می شود و به مقدار بیت کوینی که باید به این آدرس ارسال شود اضافه می شود. این دو داده، یعنی مقدار بیت کوینی که قصد داریم ارسال کنیم، و scriptPubKey در کنار هم، یک خروجی تراکنش را می سازند.

آلت کوین

Altcoin

پس از ظهور بیت کوین، شبکه غیرمتمرکز و سیستم پرداخت همتا-به-همتای آن الهام بخش پدید آمدن یک کلاس دارایی جدید شد. بازارهای کریپتوکارنسی در نتیجه موفقیت بیت کوین پدید آمدند و این بازار در حال حاضر شامل هزاران پروژه مختلف است. به این پروژه ها و کوین ها که از سال ۲۰۱۱ و به منظور از نو اختراع کردن بیت کوین و اضافه کردن ویژگی های جدید به آن بوجود آمده اند، آلت کوین گفته می شود. نخستین آلت کوین در آوریل سال ۲۰۱۱ و با به خدمت گرفتن کد

و سیستم بلاک چین بیت کوین به وجود آمد و Namecoin نام داشت.

هیچکدام از جایگزین‌های بیت کوین که از سال ۲۰۱۱ به بعد در حال معرفی شدن هستند، نتوانستند به قیمت، کاربری، و یا امنیت بیت کوین نزدیک شوند و به صورت عمومی مورد استفاده قرار گیرند. یکی از مهم‌ترین دلایل این امر متمرکز بودن این پروژه‌ها است.

ناشناس

Anonymous

ناشناس به فردی می‌گویند که هویت واقعی‌اش مشخص نیست. یک فرد ناشناس از نام مستعار استفاده می‌کند و برای انجام فعالیت‌های عمومی هویت خود را فاش نمی‌کند. ناشناس بودن و ناشناس ماندن در عصر اینترنت بسیار دشوار است. تقریباً همه خدمات بانک‌ها، کارفرمایان، رسانه‌های اجتماعی، و شرکت‌های تلفن منوط به ارائه اطلاعات هویتی شخصی است.

مدارهای مجتمع با کاربرد خاص

Application-Specific

Integrated Circuit (ASIC)

(ای‌سیک)

مدارهای مجتمع با کاربرد خاص ریزتراشه‌ای است که برای انجام یک کاربرد خاص ساخته شده است. مایکروهای ASIC بیت کوین، سخت‌افزاری هستند که این تراشه‌ها درون آن‌ها قرار گرفته است و فقط به منظور هش کردن بلاک‌های زنجیره و برای پیدا کردن یک عدد اثبات کار معتبر بکار گرفته می‌شوند. در اصل تنها کاربرد این ریزتراشه‌ها اجرای عملگر SHA-256 روی سربرگ بلاک‌های زنجیره بیت کوین است.

از آنجا که امروزه صنعت استخراج بیت کوین به یک صنعت بزرگ تبدیل شده، سختی شبکه به حدی افزایش یافته است که دیگر بکارگیری از CPU یا GPU برای استخراج بیت کوین سودآور نیست. در صنعتی که کوچکترین بهبود در کارایی ابزارهای استخراج موجب برتری می‌شود، بکارگیری از تراشه‌ای که فقط برای انجام یک کار بخصوص طراحی و ساخته شده است برای افرادی که در صنعت استخراج بیت کوین مشغول هستند دستاوردهای بزرگی به دنبال دارد. دلیل

انفجار توان هش شبکه بیت کوین نوآوری‌های سریعی است که در طول دهه گذشته در صنعت ASIC رخ داده و موجب تقویت هرچه بیشتر امنیت بیت کوین شده است.

مکتب اقتصادی اتریش **Austrian School Of Economics**

این تئوری اقتصادی در اواخر قرن نوزدهم توسط اقتصاددانان اتریشی توسعه یافت. این تئوری برای تعیین ارزش یک کالا، بر روی اهمیت کاربرد آن برای مصرف کننده تأکید دارد. این تئوری جدید ارزش توسط کارل منگر در سال ۱۸۷۱ منتشر شد. دقیقاً همان سالی که ویلیام استنلی جونز، اقتصاددان انگلیسی به طور مستقل نظریه مشابهی را منتشر کرد.

منگر معتقد بود که ارزش، یک مقوله کاملاً سلیقه‌ای است: ارزش یک محصول در توانایی آن برای برآورده ساختن نیازهای انسانی تعیین می‌شود. علاوه بر این، هرچه یک محصول فراوان‌تر باشد، برای مصارفی که از اهمیت کمتری برخوردارند مورد استفاده قرار خواهد گرفت. هرچه یک محصول کمیاب‌تر شود، مصارف کم‌اهمیتی که از آن می‌شده نیز کم‌کم منسوخ می‌شوند. (این ایده مربوط به قانون تقاضا می‌شود که می‌گوید زمانی که قیمت چیزی افزایش می‌یابد، تقاضای آن از طرف مردم کم می‌شود. این قانون یکی از مهم‌ترین قوانین اقتصاد است).

نظریه ارزش برای «معمای الماس و آب» پاسخی ارائه می‌کند. این پارادوکس توسط آدام اسمیت مطرح شد، اما خود او قادر به حل آن نبود. اسمیت به این نکته اشاره کرد که هرچند زندگی بدون آب ممکن نیست و هر انسانی می‌تواند بدون الماس به زندگی خود ادامه دهد، اما الماس از آب بسیار ارزشمندتر است. تئوری «کاربرد حاشیه‌ای» ارزش، این پارادوکس را حل می‌کند. در کل آب بسیار ارزشمندتر از الماس است و هر فرد فقط از یک مقدار مشخص از آبی که به دستش می‌رسد برای زنده ماندن استفاده می‌کند. اما چون آب در طبیعت فراوان، و الماس کمیاب است ارزش حاشیه‌ای ۱۰۰ گرم الماس از ارزش حاشیه‌ای ۱۰۰ میلی‌لیتر آب بیشتر است.

این ایده که ارزش یک کالا بر اساس کاربرد این کالا برای صاحب آن تعیین می‌شود با تئوری ارزش کارل مارکس که ادعا می‌کند ارزش هر کالایی بر اساس مقدار کاری که برای ساخت آن

انجام گرفته محاسبه می شود، در تناقض است.

B

سازگاری عقب‌رو (پساسازگاری)

Backwards Compatibility

اگر یک به‌روزرسانی روی یک سیستم انجام شود و نسخه قبلی را بلااستفاده نکند، به آن یک ارتقاء با سازگاری عقب‌رو می‌گویند. سازگاری عقب‌رو زمانی ممکن خواهد بود که یک به‌روزرسانی قوانین معتبر فعلی را در نسخه جدید، نامعتبر کند. اما اگر در یک به‌روزرسانی قوانین نامعتبر فعلی، معتبر شوند سازگاری عقب‌رو حاصل نخواهد شد. سازگاری عقب‌رو به کاربران در پذیرفتن یا نپذیرفتن تغییرات جدید، و همچنین زمان به‌کارگیری آن‌ها اختیار می‌دهد و روش پیشنهادی برای ایجاد تغییرات در سیستم‌های غیرمتمرکز و مبتنی بر اجماع است. وقتی یک به‌روزرسانی در پروتکل بیت‌کوین سازگاری عقب‌رو داشته باشد سافت فورک، در غیر این صورت هارد فورک نامیده می‌شود.

برای نمونه، لامپ‌های LED نسبت به لامپ‌های رشته‌ای معمولی برتری‌های زیادی دارند. با این حال می‌توان لامپ‌های LED را در سوکت‌های قدیمی لامپ‌های رشته‌ای پیچاند و از آن‌ها استفاده کرد. بنابراین ارتقاء لامپ‌های موجود در منازل موجب بلااستفاده شدن لامپ‌های رشته‌ای نخواهد شد.

توسعه‌دهندگان پروتکل بیت‌کوین همواره در حین طراحی و اجرای تغییرات و قابلیت‌های جدید تلاش می‌کنند تا این به‌روزرسانی‌ها از روش سازگار با قوانین گذشته انجام شود تا کاربران مجبور به پذیرش قوانین جدید نباشند. برای نمونه یکی از مهم‌ترین به‌روزرسانی‌های قوانین شبکه بیت‌کوین یعنی سکوئیت در سال ۲۰۱۷ از راه سافت فورک روی شبکه اجرا شد.

کُدبندی بیس-۵۸

Base58

یک روش کُدبندی است که از ۵۸ کاراکتر از الفبای انگلیسی شامل حروف کوچک و بزرگ A-Z و ارقام ۹-۱ استفاده می‌کند. این روش کُدبندی برای جلوگیری از سردرگمی کاربران، عدد

صفر، حرف 0 بزرگ، حرف I بزرگ، و حرف l کوچک را حذف کرده است.

یکی از گونه‌های این روش کدبندی، روش بیس-۵۸ با قابلیت جمع‌آزمایی است که برای نمایش آدرس‌های قدیمی بیت‌کوین و کلیدهای خصوصی در قالب WIF استفاده می‌شود. بیس-۵۸ با قابلیت جمع‌آزمایی با بیس-۵۸ کاملاً یکسان است، فقط یک جمع‌آزمای ۴ بایتی به انتهای آن، و یک پیشوند برای مشخص کردن نسخه به ابتدای آن اضافه شده است. در این صورت پیشوند نمایانگر اصل داده کدبندی شده است. برای نمونه آدرس‌های P2PKH با ۱ شروع می‌شوند، آدرس‌های P2SH با ۳ شروع می‌شوند، و کلیدهای خصوصی در قالب WIF دارای پیشوند ۵ هستند.

کدبندی بیس-۶۴^۸

Base64

روشی است که برای کدبندی تراکنش‌هایی که به صورت ناقص امضا شده‌اند (PSBT) به کار گرفته می‌شود. این روش شامل ۶۴ کاراکتر الفبای انگلیسی، یعنی همه حروف بزرگ و کوچک، ارقام ۰-۹، و کاراکترهای + و / است. این روش با توجه به تعداد کاراکترهای زیادی که به خدمت می‌گیرد قادر است داده‌ها را به صورت بسیار بهینه نمایش دهد، اما خوانایی پایینی دارد. بنابراین این روش اغلب برای کدبندی داده‌هایی به کار می‌رود که قرار نیست توسط انسان‌ها خوانده شوند و معمولاً از روش اسکن کدهای QR بین دستگاه‌ها منتقل می‌شود.

ارسال گروهی بیت‌کوین

Batching

ارسال گروهی بیت‌کوین به معنی ادغام تراکنش‌های جداگانه در یک تراکنش، با چند خروجی است. از آنجا که کارمزد تراکنش‌های بیت‌کوین براساس سائز تراکنش محاسبه می‌شود، ادغام چندین تراکنش در یک تراکنش واحد می‌تواند سائز تراکنش را کاهش، و موجب صرفه‌جویی در هزینه‌ها شود. برای نمونه اگر آوا بخواهد به بابک ۰/۵ بیت‌کوین، به حمید ۰/۳ بیت‌کوین، و به داوود ۰/۲ بیت‌کوین ارسال کند، می‌تواند بجای ساختن ۳ تراکنش که هر کدام ۲ خروجی دارند - یکی برای پرداخت و دیگری باقیمانده، - یک تراکنش با یک ورودی ۱ بیت‌کوین و سه خروجی بسازد.

مزایای ادغام تراکنش‌ها در مقیاس‌های بزرگ‌تر افزایش می‌یابد. برای نمونه، یک صرافی می‌تواند درخواست برداشت ۱۰۰ نفر از مشتریان خود را با ساختن ۱۰۰ تراکنش جداگانه انجام دهد، و همچنین می‌تواند یک تراکنش با صد خروجی بسازد. گزینه دوم موجب صرفه‌جویی قابل توجهی در کارمزد تراکنش می‌شود.

کُدبندی بِش-۳۲

Bech32

روشی برای کُدبندی آدرس‌های سگویت و درخواست‌های پرداخت روی شبکه لایت‌نینگ است. این روش از ۳۲ کاراکتر الفبای انگلیسی؛ حروف کوچک a-z و اعداد ۰-۹، و حذف عدد ۱ و حروف i, b, و o - به منظور جلوگیری از سردرگمی کاربران، - تشکیل شده است. این روش کُدبندی شامل مکانیزم تشخیص خطا است.

کُدبندی بِش-۱۳۲م

Bech32m

این روش کُدبندی درواقع نسخه اصلاح شده روش بش-۳۲ است و تقریباً هیچ تفاوتی با آن ندارد. این روش خطای موجود در مکانیزم تشخیص خطای بش-۳۲ را برطرف و امنیت را با تغییر مقدار ثابتی مورد استفاده قرار گرفته بود، بالاتر می‌برد. روش بش-۱۳۲م برای کُدگذاری آدرس‌های نسخه ۱ سگویت که توسط ارتقاء تپ‌روت معرفی خواهد شد، مورد استفاده قرار خواهد گرفت.

باینری

Binary

دستگاه اعداد دودویی یا باینری سیستمی است که فقط از دو عدد استفاده می‌کند: صفر و یک. کامپیوترها در دستگاه اعداد دودویی کار می‌کنند، به این معنی که آن‌ها داده‌ها را با استفاده از صفر و یک محاسبه و ذخیره می‌کنند. به عبارت دیگر ورودی‌هایی مانند حرکت ماوس، فشار دادن دکمه‌های صفحه کلید و هرگونه اطلاعات دیگری که توسط کامپیوترها پردازش می‌شود در پایین‌ترین سطح به سیستم دودویی تبدیل می‌شود.

از آنجا که طول اعداد باینری از اعداد ده‌دهی (سیستم رایج نمایش اعداد) یا هگزادسیمال بلندتر است، معمولاً آن‌ها را برای سهولت در خواندن و نوشتن به سیستم اعشاری یا هگزادسیمال تبدیل می‌کنند. به عنوان نمونه، عدد ۷۵ را می‌توان به صورت ۰۱۰۰۱۰۱۱ در سیستم باینری، و 4b در سیستم هگزادسیمال نمایش داد.

BIP39 (Mnemonic Phrases)

بیپ-۳۹ (کلمات بازیابی)

بیپ-۳۹، پیشنهاد بهود بیت‌کوین با کُد ۳۹ است و استاندارد کلمات بازیابی در آن مطرح شده است. کلمات بازیابی روشی استاندارد برای تبدیل بذر کلید خصوصی بیت‌کوین به مجموعه‌ای ۱۲ تا ۲۴ کلمه‌ای است. بنابراین برای بازیابی همه کلیدهای خصوصی یک کیف پول بیت‌کوین، در اختیار داشتن این کلمات به تنهایی کفایت می‌کند.

در حالی که استاندارد بیپ-۳۹ تقریباً توسط همه کیف پول‌های محبوب بیت‌کوین مورد پذیرش قرار گرفته است، اما همچنان در نرم‌افزار بیت‌کوین کُر پیاده‌سازی نشده و از نظر مهندسی نقاط ضعفی دارد. با این حال هیچ‌گونه نقطه ضعف امنیتی در آن نیست و می‌توان از آن به عنوان راهی مناسب برای پشتیبان‌گیری از کیف پول‌های بیت‌کوین استفاده کرد.

Bit

بیت

نام اختصاری «رقم دوتایی» است و مقدار آن یا یک است یا صفر. یک بیت کوچکترین واحد داده‌های دیجیتالی است. همه داده‌های کامپیوتری به صورت بیت ذخیره می‌شوند. بیت‌ها در دسته‌های ۸ تایی با یکدیگر گروه‌بندی می‌شوند، بنابراین هر بایت از ۸ بیت تشکیل شده است.

ممکن است شما با مگابایت (MB) و گیگابایت (GB) آشنا باشید. یک مگابایت یک میلیون بایت یا ۸ میلیون بیت است. به همین ترتیب، یک گیگابایت یک میلیارد بایت یا ۸ میلیارد بیت است. این بدان معناست که وقتی سائز یک فایل ۱ مگابایت باشد، یعنی این فایل از ۸ میلیون صفر و یک تشکیل شده است.

گاهی اوقات، بیت به یکی از واحدهای شمارش بیت کوین اشاره دارد. در این صورت هر بیت، ۱۰۰ ساتوشی یا ۱ میلیونوم بیت کوین است. این واحد اکنون با گذشت زمان و به دلیل استفاده نشدن تقریباً منسوخ شده است.

بیت کوین

Bitcoin

بیت کوین یک پول شبیه به بقیه پولهای رایج در دنیا است با این تفاوت کلیدی که تحت نظارت هیچ بانک مرکزی و تحت کنترل هیچ فرد یا نهادی نیست. شبکه بیت کوین یک شبکه همتا-به-همتا، و مکانیسم اجماع آن بر پایه اثبات کار و یک دفتر کل غیرمتمرکز به نام بلاک چین است. بیت کوین در تاریخ ۳۱ اکتبر سال ۲۰۰۸ (مطابق با دهم آبان ۱۳۸۷ خورشیدی) توسط خالق ناشناس آن یعنی ساتوشی ناکاموتو معرفی، و شبکه آن نیز در تاریخ ۳ ژانویه سال ۲۰۰۹ راه اندازی شد.

عرضه بیت کوین به ۲۱ میلیون کوین محدود، سیاست پولی آن ثابت، و از قبل برنامه ریزی شده است. هر چهار سال، نرخ عرضه آن به نصف کاهش پیدا می کند و در نهایت به صفر می رسد. این یکی از خصوصیات منحصر به فرد بیت کوین در مقایسه با دیگر پروژه های آلت کوین است که عرضه آنها به صورت مداوم، غیر قابل پیش بینی، و بی حد و حصر ادامه دارد.

بیت کوین تحت کنترل یک نهاد مرکزی نیست. به جای به خدمت گرفتن معماری سرویس دهنده-سرویس گیرنده و قرار دادن یک پایگاه داده مرکزی در مرکز شبکه و فراهم کردن داده های مورد نیاز به کاربران شبکه، هریک از کاربران حاضر در شبکه بیت کوین از یک نسخه از پایگاه داده دفتر کل حسابداری بیت کوین بر روی دستگاه شان نگهداری می کنند. این قابلیت به کاربران این امکان را می دهد که موجودی ها و تاریخچه نقل و انتقال همه بیت کوین ها را به طور مستقل بررسی کنند. زنجیره بلاک های بیت کوین به صورتی طراحی شده است که فقط می توان به آن بلاک های جدید را اضافه کرد و به هیچ وجه نمی توان بلاک های قدیمی را تغییر داد یا حذف کرد.

بیت کوین

bitcoin

از آنجا که بیت کوین نام پروتکل و همچنین نام واحد پولی بیت کوین است، بزرگ یا کوچک نوشتن حرف اول آن بستگی به بستر معنایی متن دارد. بیت کوین با حرف اول بزرگ اشاره به شبکه بیت کوین و کلاس دارایی دارد. از طرف دیگر بیت کوین با حرف اول کوچک به واحد پولی و همچنین مقادیری که در کیف پول‌ها نمایش، و جابجا می‌شود اشاره دارد.

بیت کوین کُر

Bitcoin Core

بیت کوین کُر رایج‌ترین پیاده‌سازی پروتکل بیت کوین است و سایر پیاده‌سازی‌ها برای اطلاع از روش نگهداری از قوانین اجماع و همچنین روش به‌روزرسانی، به آن مراجعه می‌کنند. اکثر کاربران برای دریافت سورس بیت کوین آن را دانلود می‌کنند. بیت کوین کُر نرم‌افزاری برای نود شبکه و یک کیف پول برای کاربران فراهم می‌کند. البته اکثر کاربران ترجیح می‌دهند از آن فقط به‌عنوان نرم‌افزار نود استفاده کنند و برای کیف پول، نرم‌افزارهای دیگری را به خدمت بگیرند. جایگزین‌های دیگری نیز برای این پیاده‌سازی وجود دارد، اما این پیاده‌سازی همچنان از نظر محبوبیت و استفاده کاربران غالب است. هرکس مایل به اجرای آن به‌عنوان نرم‌افزار نود شبکه باشد می‌تواند از طریق صفحه گیت‌هاب یا وب‌سایت این پروژه، به آن دسترسی پیدا کند.

بیت کوین کُر توسط ساتوشی ناکاموتو ایجاد شده است و با وجود اینکه مالکیت آن به توسعه‌دهندگان این نرم‌افزار منتقل شده و قابلیت‌های زیادی به آن اضافه شده است، نسخه آخر و نسخه اصلی ساتوشی همچنان با یکدیگر سازگار هستند.

بیت کوین کُر یک نرم‌افزار منبع باز (اپن سورس) است. این بدان معناست که هرکس می‌تواند کد آن را تکثیر و به دلخواه خود ویرایش کند. اگر یک توسعه‌دهنده قصد دارد کد بیت کوین را بهبود بخشد می‌تواند تغییرات ایجاد شده را منتشر، و پیشنهاد ادغام شدن آن‌ها را به توسعه‌دهندگان پروژه بدهد. بسیاری از توسعه‌دهندگان از طریق نوشتن، بازبینی، و بحث و بررسی در مورد قسمت‌های مختلف سورس این نرم‌افزار در آن مشارکت می‌کنند. با این حال هیچ‌گونه مرجع مشخصی برای تأمین منابع مالی توسعه‌دهندگان این نرم‌افزار وجود ندارد. در عوض شرکت‌ها و افرادی که در زمینه بیت کوین فعالیت می‌کنند بخشی از هزینه‌های این افراد را از طریق کمک‌های مالی و کمک‌های

بلاعوض تأمین می کنند.

پیاده سازی های بیت کوین

Bitcoin Implementations

یک پیاده سازی بیت کوین در واقع یک برنامه نرم افزاری است که کامپیوتر شما را به یک نود در شبکه بیت کوین تبدیل، و با دیگر نودهای حاضر در شبکه تعامل برقرار می کند. چندین پیاده سازی مختلف از نرم افزار بیت کوین وجود دارد که به زبان های برنامه نویسی مختلف نوشته شده اند. هر کس می تواند کد آن را تکثیر و تغییر دهد یا عمل کرد آن را شبیه سازی کند، زیرا بیت کوین یک پروژه منبع باز (اپن سورس) است. این امر به جای آسیب رساندن به امنیت و کارایی بیت کوین، موجب تقویت آن می شود.

هر پیاده سازی، طراحی و ویژگی های متفاوتی نسبت به دیگران ارائه می کند، اما در نهایت همه آنها می بایست برای حفظ یکپارچگی شبکه بیت کوین روی قوانین اجماع پروتکل بیت کوین توافق کنند. به عنوان مثال، پیاده سازی های مختلف می توانند از انواع کیف پول ها، اشکال متفاوت تراکنش ها، برآورد هزینه تراکنش، یا انتخاب کوین ها برای ایجاد تراکنش ها استفاده کنند اما همه آنها باید قوانین یکسانی را در مورد اعتبار بلاک ها، تراکنش ها، و امضاهای دیجیتال اعمال کنند. در حالی که امروزه پیاده سازی مختلفی از پروتکل بیت کوین وجود دارد، نرم افزار بیت کوین گری یعنی پیاده سازی اصلی ای که توسط ساتوشی ناکاموتو در سال ۲۰۰۸ ایجاد شد، نسبت به دیگر پیاده سازی ها غالب است و توسط افراد بیشتری مورد استفاده قرار می گیرد. دیگر پیاده سازی ها شامل نرم افزارهای Bitcoin Knots، bcoin، و btcd است.

پیشنهاد بهبود بیت کوین (بیپ) Bitcoin Improvement Proposal (BIP)

پیشنهاد بهبود بیت کوین یک پیشنهاد رسمی برای بهبود شبکه بیت کوین است. ارتقاء کد و بهبود امنیت شبکه بیت کوین از این کانال در سورس کد بیت کوین وارد می شوند. به روزرسانی های پروتکل بیت کوین از قبیل سگویت، کیف پول های سلسله مراتبی پیش بینی پذیر، تراکنش هایی که به صورت ناقص امضاء شده اند، و موارد مشابه دیگر، همگی قبل از اینکه مورد پذیرش قرار بگیرند و

به قوانین شبکه وارد شوند، از این روش معرفی، و تحت بحث و بررسی کاربران بیت کوین قرار گرفته‌اند. با این حال همه این پیشنهادها قصد تغییر کُد یا قوانین اجماع بیت کوین را ندارند. برخی از آن‌ها، مانند استاندارد بیپ-۳۹ قواعدی را به منظور تهیه پشتیبان از کلمات بازیابی تعیین می‌کنند و در سایر پروژه‌های مرتبط با بیت کوین کاربرد دارند.

تغییرات جزئی‌تر مانند برطرف کردن اشکالات نرم‌افزاری، بهبود فرمت کُد، یا ایجاد بهبود جزئی در کارایی کُد، از این کانال انجام نمی‌شود. این تغییرات به صورت مستقیم و به عنوان پیشنهاد تغییر کُد بر روی مخزن سورس بیت کوین ارسال می‌شوند و در همان بخش مورد بحث و بررسی قرار می‌گیرند.

نود بیت کوین

Bitcoin Node

یک عضو گسسته از شبکه همتا-به-همتای بیت کوین است که با همتایان خود در شبکه ارتباط برقرار می‌کند و یک شبکه تشکیل می‌دهد. یک نود بیت کوین به هر کامپیوتری گفته می‌شود که یکی از پیاده‌سازی‌های بیت کوین را اجرا می‌کند و همه یا بخشی از زنجیره بیت کوین را در خود ذخیره می‌کند. نودها تراکنش‌های کاربران و همچنین بلاک‌های ساخته شده توسط ماینرها را میان یکدیگر دست‌به‌دست، و اعتبار آن‌ها را می‌سنجند. اگر نرم‌افزار همه نودهای شبکه با یکدیگر سازگاری داشته باشد، می‌توان گفت که نودهای شبکه به اجماع رسیده‌اند.

به منظور محافظت از قوانین اجماع، جلوگیری از اجرای گداهای مخرب، و همچنین جلوگیری از ایجاد تغییرات در ترتیب بلاک‌ها در زنجیره بیت کوین، تعداد نودهای شبکه بیت کوین از اهمیت بالایی برخوردار است.

زبان اسکریپت‌نویسی بیت کوین

Bitcoin Script

به زبان اسکریپت‌نویسی بیت کوین «اسکریپت» می‌گویند. تمام اسکریپت‌های بیت کوین به زبان «اسکریپت» نوشته شده‌اند. این زبان بسیار ساده و ابتدایی است و از نظر تئوری محاسباتی، تورینگ

کامل نیست. این بدان معنی است که این زبان از چندین عملگر منطقی از جمله حلقه‌ها پشتیبانی نمی‌کند. این کار باعث می‌شود اطمینان داشته باشیم که هیچگونه اسکرپیت خرابکارانه‌ای نمی‌تواند از طریق اجرای عملگرهایی که به توان محاسباتی بالایی نیاز دارند به نودهای شبکه همتا-به-همتا آسیب برساند.

از این زبان تقریباً به‌طور انحصاری برای قفل، و آزاد کردن بیت کوین‌های قفل شده استفاده می‌شود، و برای ساخت اپلیکیشن‌ها و اجرای آن‌ها روی زنجیره بیت کوین مورد استفاده قرار نمی‌گیرد. سادگی اسکرپیت، موجب افزایش امنیت بیت کوین می‌شود.

تمام تراکنش‌های بیت کوین برای تعریف روش باز شدن قفل بیت کوین‌هایی که روی یک خروجی تراکنش قرار دارند، از زبان اسکرپیت استفاده می‌کنند. به عبارت دیگر، در یک تراکنش، این اسکرپیت است که مشخص می‌کند بیت کوین ارسال شده متعلق به چه کسی است. بیت کوین دارای انواع اسکرپیت‌های مختلف است ولی یکی از معروف‌ترین آن‌ها P2PKH است که درواقع آدرس‌هایی هستند که با عدد ۱ شروع می‌شوند. انواع دیگر اسکرپیت می‌توانند قوانین پیچیده‌تری تولید کنند، مانند آدرس‌های چند امضایی. در این شرایط برای نقل و انتقال بیت کوینی که به یک آدرس چند امضایی ارسال شده، نیاز به امضای دیجیتال داریم که توسط چندین کلید خصوصی مختلف تولید شده باشد.

یکی دیگر از انواع اسکرپیت، اسکرپیت‌های سگویی P2WPKH و P2WSH هستند که به کارگیری آن‌ها موجب صرفه‌جویی در کارمزد تراکنش خواهد شد.

Bitcoin Whitepaper

وایت پیپر بیت کوین

وایت پیپر یک مقاله علمی برای معرفی یک ایده جدید است، یا موضوعی را برای بحث مطرح می‌کند. وایت پیپر بیت کوین درواقع بیت کوین را به‌عنوان «سیستم پول نقد بر پایه یک سیستم همتا-به-همتا» معرفی می‌کند که «نیازی به اعتماد اشخاص ثالث ندارد». ساتوشی ناکاموتو وایت پیپر بیت کوین را در ۳۱ اکتبر سال ۲۰۰۸ در گروه ایمیلی متخصصین رمزنگاری و سایف‌پانک‌ها منتشر

کرد.

بیت کوین کیوت

Bitcoin-Qt

نام رابط گرافیکی کاربر و بخشی از مجموعه نرم‌افزاری بیت کوین گر است. این نرم‌افزار نود و کیف پول بیت کوین را در قالب فرم‌های گرافیکی بر روی صفحه‌نمایش نشان می‌دهد. پسوند QT از نام ابزار Qt Toolkit Gui مشتق شده که برای ساخت نرم‌افزار بیت کوین کیوت مورد استفاده قرار گرفته است.

بلاک

Block

یک بلاک مجموعه‌ای از تراکنش‌های معتبری است که در شبکه بیت کوین منتشر شده‌اند. این بلاک‌ها بر اساس تسلسل زمانی به یکدیگر متصل هستند و یک زنجیره را تشکیل می‌دهند. بلاک‌های بیت کوین در حال حاضر می‌توانند تا حدود ۲,۷۰۰ تراکنش را در خود جای دهند. این تعداد ممکن است در آینده با پیشرفت‌های پروتکل بیت کوین بیشتر شود.

یک بلاک تنها زمانی معتبر است و می‌تواند به زنجیره بیت کوین اضافه شود که مقدار هش آن در چهارچوب اثبات کار مورد پذیرش در شبکه بیت کوین باشد و همچنین هش بلاک قبلی را نیز در سربرگ خود داشته باشد. گنجاندن هش بلاک قبلی در یک بلاک تضمین می‌کند که تغییر یک بلاک قطعاً موجب تغییر بلاک‌های بعدی در زنجیره بلاک بیت کوین خواهد شد. این ویژگی به دلیل ماهیت توابع هش است که قطعی و تصادفی هستند. این سیستم موجب می‌شود زنجیره بلاک بیت کوین تغییرناپذیر شود.

به عنوان مثال، اگر تراکنشی در بلاک شماره ۴۰۰ تغییر کند، هش این بلاک تغییر خواهد کرد و در پی آن عدد اثبات کار بلاک شماره ۴۰۰ دیگر معتبر نخواهد بود. ولی این مسأله به اینجا ختم نمی‌شود چرا که بلاک شماره ۴۰۱ نیز نامعتبر خواهد شد، زیرا پارامتر هش بلاک قبلی در بلاک ۴۰۱ دیگر با هش بلاک شماره ۴۰۰ مطابقت ندارد. این تغییر به صورت آشنایی به سمت جلو

حرکت می کند و ارتباط همه بلاک هایی که پس از بلاک شماره ۴۰۰ آمده اند را از یکدیگر قطع می کند. این ویژگی تضمین می کند که پس از اضافه شدن یک بلاک به زنجیره بلاک های بیت کوین، دیگر نمی توان آن بلاک یا هریک از تراکنش های موجود در آن را تغییر داد.

بلاک اکسپلورر (کاوشگر بلاک) **Block Explorer**

بلاک اکسپلورر سرویسی است که عموم افراد را قادر می سازد بلاک ها، آدرس ها، و تراکنش های زنجیره بیت کوین را مرور، و از وضعیت آن ها مطلع شوند. زنجیره بلاک های بیت کوین در دسترس عموم افراد قرار دارد. ده ها هزار نود در شبکه بیت کوین یک نسخه از زنجیره بلاک های بیت کوین را در خود ذخیره کرده اند و این موضوع صاحبان آن ها را قادر می سازد تا هریک از تراکنش ها و بلاک هایی که در شبکه بیت کوین منتشر می شود را دریافت کنند، اعتبار آن ها را بسنجند، و موجودی بیت کوین خود را محاسبه کنند. یک بلاک اکسپلورر این خدمات را برای افرادی که نود شخصی خود را اجرا نمی کنند فراهم می کند.

اما این سهولت به قیمت از بین رفتن حریم خصوصی و اعتماد به یک شخص ثالث تمام می شود. اغلب بلاک اکسپلوررها سرویس خود را در قالب یک وبسایت به کاربران ارائه می کنند و ممکن است داده های مربوط به آدرس IP کاربران، مکان فیزیکی، و آدرس های بیت کوین اعلام گرفته شده توسط کاربران سایت خود را جمع آوری کنند و این موضوع به شدت به حریم خصوصی کاربران این وبسایت ها لطمه می زند. برخی از بلاک اکسپلوررها برای حل این مشکل و حفظ حریم خصوصی، به کاربران خود اجازه می دهند که نرم افزار این سرویس را به صورت محلی و بر روی نود خود اجرا کنند.

برای امتحان یک بلاک اکسپلورر و خدماتی که ارائه می کند، از سایت mempool.space بازدید، و فهرست کامل بلاک های شبکه بیت کوین و تراکنش های آن ها را مرور کنید. پیشنهاد می شود برای حفظ حریم خصوصی، آدرس ها و تراکنش های شخصی خود را وارد این سایت نکنید.

یک بلاک در زنجیره بیت کوین مجموعه‌ای از تراکنش‌ها است. این بلاک همچنین شامل فراداده‌ای است که خلاصه‌ای از بلاک مورد نظر ارائه می‌کند. این فراداده، سربرگِ بلاک نام دارد. سربرگِ بلاک شامل اطلاعات مختلفی از بلاک مورد نظر است:

- شماره بلاک در طول زنجیره: عددی است که نشان می‌دهد قبل از بلاک مورد نظر، چه تعداد بلاک وجود دارد.
- هش بلاک: نماینده عدد اثبات کار است.
- هش بلاک قبل: قرار گرفتن این مقدار در سربرگِ بلاک غیرقابل تغییر بودن بلاک‌های قبلی را تضمین می‌کند.
- برچسب زمان: نشان می‌دهد که بلاک مورد نظر در چه زمانی منتشر شده است.
- ریشهٔ مرکب: هش همه تراکنش‌هایی است که در بلاک مورد نظر قرار گرفته است.
- سختی شبکه: این مقدار به روش خاصی گدبندی می‌شود و با نام "bits" در سربرگِ بلاک قرار می‌گیرد.
- نانس: یک عدد تصادفی که به ماینرها این اجازه را می‌دهد که با تغییر آن، عدد اثبات کار معتبری برای بلاک پیدا کنند.

سربرگِ بلاک نقش چکیده آن را ایفا می‌کند و با توجه به سائز کوچکی که دارد می‌تواند سریع‌تر از خودِ بلاک بین نودهای شبکه منتقل و پردازش شود. ماینرها برای پیدا کردن عدد اثبات کار متغیرهای مجاز در سربرگِ بلاک را تغییر می‌دهند و درواقع فقط با سربرگِ بلاک سر و کار دارند و آن را هش می‌کنند.

این روش بسیار بهینه است، زیرا هرچه اطلاعاتی که می‌بایست هش شود بیشتر باشد -مانند هزاران تراکنشی که در یک بلاک قرار دارد- به زمان و منابع بیشتری برای این کار نیاز خواهد بود. اگر ماینرها مجبور بودند همه اطلاعات بلاک را برای پیدا کردن عدد اثبات کار هش کنند، در این صورت ممکن بود برای بالابردن بهره‌وری خود، بلاک‌های خالی تولید کنند و این مسأله منجر به

پایین آمدن ظرفیت پردازش تراکنش‌ها در شبکه بیت کوین می‌شد.

Block Height

شماره بلاک در طول زنجیره

یک زنجیره بلاک در واقع از بهم پیوستن بلاک‌هایی تشکیل شده است که بر اساس ترتیب زمانی به یکدیگر متصل، و غیرقابل تغییر باشند. بلاک‌هایی که بعد از بلاک شماره صفر - که به بلاک پیدایش نیز معروف است - آمده‌اند، همگی به صورت صعودی شماره گذاری می‌شوند. این شماره، در واقع شماره بلاک در طول زنجیره است.

آخرین شماره بلاک در واقع چیزی نیست جز تعداد بلاک‌های زنجیره بیت کوین منهای عدد یک. از این عدد همچنین می‌توان برای اشاره به یک زمان مشخص بر روی زنجیره بلاک استفاده کرد. برای نمونه، رویداد نصف شدن پاداش ساختن یک بلاک هر ۲۱۰,۰۰۰ بلاک اتفاق می‌افتد. علاوه بر این می‌توان با به کارگیری این شماره، بر روی تراکنش‌های بیت کوین قفل‌های زمانی بخصوصی ایجاد کرد.

Block Reward

پاداش بلاک

یک ماینر با ساخت یک بلاک معتبر اجازه پیدا می‌کند مقدار مشخصی بیت کوین را در قالب یارانه ساخت بلاک خلق و به آدرس خود منتقل کند. همه تراکنش‌هایی که در شبکه بیت کوین منتشر می‌شوند نیز باید مقداری بیت کوین به عنوان کارمزد به ماینرها پرداخت کنند. پاداش ساخت بلاک، در واقع حاصل جمع این دو مقدار است. از آنجا که یارانه ساخت بلاک هر چهار سال نصف می‌شود، کارمزد تراکنش‌ها در گذر زمان بخش بیشتری از پاداش بلاک را به خود اختصاص خواهد داد. واژه پاداش بلاک و یارانه بلاک اغلب بجای یکدیگر بکار گرفته می‌شوند.

پاداش بلاک در یک تراکنش ویژه به نام کوین بیس به ماینر آن پرداخت می‌شود. این تراکنش ویژه اولین تراکنش در فهرست تراکنش‌های بلاک است و ورودی ندارد. ماینرها می‌بایست برای خرج کردن خروجی این تراکنش ۱۰۰ بلاک صبر کنند.

وزن بلاک مقیاسی برای اندازه‌گیری سائز بلاک است و در واحد وزن اندازه‌گیری می‌شود. پروتکل بیت کوین برای محدود کردن تعداد تراکنش‌هایی که ماینرها می‌توانند در یک بلاک قرار دهند، سائز بلاک‌ها را به ۴ میلیون در واحد وزن محدود می‌کند. این محدودیت به منظور جلوگیری از رشد سریع سائز زنجیره بلاک بیت کوین است. اگر سائز زنجیره بلاک به قدری زیاد باشد که کاربران قادر به اجرای فول نود بر روی دستگاه‌های معمولی خود نباشند، غیرمتمرکز بودن بیت کوین به خطر می‌افتد.

این مقیاس در سال ۲۰۱۷ به همراه ارتقاء سگویت به قوانین پروتکل بیت کوین اضافه شد. قبل از سگویت تنها محدودیت سائز بلاک ۱ مگابایت بود که در مقیاس بایت سنجیده می‌شد و سائز بلاک نام داشت.

زنجیره بلاک یک ساختار داده‌ای است که بیت کوین بر پایه آن بنا شده است. همانطور که از نام آن برمی‌آید، زنجیره بلاک درواقع لیستی از بلاک‌ها است. هریک از این بلاک‌ها حاوی داده است. در زنجیره بلاک بیت کوین، بلاک‌ها حاوی تراکنش‌های کاربران هستند که برای یکدیگر بیت کوین ارسال می‌کنند.

زنجیره بلاک بیت کوین را می‌توان به‌عنوان یک دفترکل حسابداری دیجیتال در نظر گرفت که از حساب‌های همه کاربران بیت کوین در شبکه نگهداری می‌کند. این زنجیره بلاک به‌مانند کتابی است که بایگانی همه تراکنش‌هایی که تابحال روی شبکه بیت کوین انجام شده را ذخیره می‌کند. بنابراین هر بلاک، به‌مانند صفحه جدیدی است که برای به‌روزرسانی وضعیت حساب‌های کاربران شبکه، به این کتاب اضافه می‌شود. زنجیره بلاک شبکه بیت کوین عمومی است و هزاران نود بیت کوین یک نسخه از این دفترکل حسابداری را در خود ذخیره می‌کنند، بنابراین شبکه بیت کوین یک شبکه غیرمتمرکز است.

یکی از ویژگی‌های خاص یک زنجیرهٔ بلاک این است که تغییرناپذیر است. پس از اضافه شدن یک بلاک به این زنجیره، تغییر آن بسیار دشوار است. همانطور که بلاک‌های بیشتری به این زنجیره اضافه می‌شوند، ایجاد تغییر در بلاک‌های قبلی عملاً غیرممکن می‌شود.

بی‌تی‌سی

BTC

نماد بیت‌کوین است. برای نمونه یک بیت‌کوین با نماد 1BTC نمایش داده می‌شود. یک بیت‌کوین به ۱۰۰,۰۰۰,۰۰۰ واحد کوچکتر به نام ساتوشی یا sats بخش‌پذیر است. یک ساتوشی در قراردادهای هوشمند شبکهٔ لایت‌نینگ -لایهٔ بیرونی زنجیرهٔ اصلی بیت‌کوین- به ۱,۰۰۰ واحد کوچکتر تقسیم می‌شود. بنابراین بیت‌کوین روی شبکهٔ لایت‌نینگ ۱,۰۰۰ برابر بخش‌پذیرتر از شبکهٔ اصلی است. اگرچه باید این نکته را در نظر گرفت که واحد میلی ساتوشی روی زنجیرهٔ اصلی بیت‌کوین تعریف نشده است.

بایت

Byte

یک بایت داده‌ای است که از ۸ بیت تشکیل شده است. برای خوانایی هرچه بیشتر، بجای استفاده از سیستم باینری که پیشوند 0b دارد، بایت در سیستم هگزادسیمال به نمایش درمی‌آید و پیشوند 0x دارد. دادهٔ تراکنش‌های بیت‌کوین، اسکرپیت‌ها، کلیدهای عمومی، و بلاک‌ها مجموعه‌ای از بایت هستند که در قالب هگزادسیمال نمایش داده می‌شوند.

تاب‌آوری در برابر خطای بیزانس

Byzantine Fault Tolerance

تاب‌آوری در برابر خطای بیزانس یک ویژگی در سیستم‌های غیرمتمرکزی است که هر کس می‌تواند بدون کسب اجازه از آن‌ها استفاده کند. این سیستم‌ها قادر به شناسایی و مردود کردن اطلاعات نادرست و ناصحیح هستند. سیستمی که در برابر خطای بیزانس تاب‌آوری دارد، درواقع توانسته مسألهٔ ژنرال‌های بیزانس را حل کرده و قادر است در مقابل حملات سیبیل ایستادگی کند.

در یک سیستم غیرمتمرکز که برای استفاده از آن نیاز به کسب مجوز نیست، هر کس می‌تواند به شبکه پیوندد و به انتشار اطلاعات بپردازد. اگر این سیستم در برابر خطای بیزانس تاب‌آوری نداشته باشد، هر عضو این شبکه می‌تواند اطلاعات نامعتبری را به شبکه ارسال، و اعتبار آن را تضعیف کند. در مورد بیت‌کوین، یک نود می‌تواند به شبکه پیوندد و اقدام به انتشار بلاک‌ها و تراکنش‌ها کند. به عنوان مثال، یک نود می‌تواند دو تراکنش در شبکه منتشر، و قصد داشته باشد که یک کوین را دو بار خرج کند. بنابراین در شبکه بیت‌کوین نودها می‌بایست راهی برای تعیین اعتبار داده‌هایی که از دیگر نودها دریافت می‌کنند در اختیار داشته باشند.

شبکه بیت‌کوین در برابر خطای بیزانس تاب‌آوری دارد زیرا هریک از نودها قادرند اعتبار تراکنش‌ها و بلاک‌ها را به‌طور مستقل و به‌صورت عینی (غیر سلیقه‌ای) بسنجند. اگر یک نود بلاک‌ها یا تراکنش‌های نامعتبری را منتشر کند، دیگر نودهای حاضر در شبکه آن‌ها را تشخیص می‌دهند و مردود می‌کنند و از وارد شدن تراکنش‌های نامعتبر به زنجیره بلاک بیت‌کوین جلوگیری می‌کنند. قوانین پروتکل بیت‌کوین برای اعتبارسنجی تراکنش‌ها و بلاک‌ها بسیار شفاف است و هیچ‌گونه ابهامی در آن وجود ندارد.

مسئله ژنرال‌های بیزانس

Byzantine Generals Problem

این مسئله شرح می‌دهد که دستیابی به یک توافق مطمئن، از راه نظریه بازی‌ها در یک شبکه غیرمتمرکز کار بسیار دشواری است. برای حل این مشکل همه اعضای شبکه باید برای تعیین حقیقت بر روی روشی که نیازمند اعتماد به هیچ موجودیتی ندارد، با یکدیگر توافق کنند.

می‌توان این مسئله را به شرایطی تشبیه کرد که در آن تعدادی از ژنرال‌های جنگی بیزانس، شهری را محاصره کرده‌اند. شهر در محاصره آن‌ها است، اما برای تعیین زمان حمله باید یک تصمیم جمعی بگیرند. اگر همه ژنرال‌ها در یک زمان حمله کنند برنده جنگ خواهند بود، اما اگر زمان حمله آن‌ها با یکدیگر متفاوت باشد، جنگ را خواهند باخت. ژنرال‌ها هیچ‌گونه کانال ارتباطی امنی با یکدیگر ندارند، زیرا هر پیامی که ارسال یا دریافت می‌کنند ممکن است توسط مدافعان شهر متوقف، یا حتی از جانب آن‌ها فرستاده شده باشد.

بیت کومین مسأله ژنرال‌های بی‌زانس را از طریق پیاده‌سازی سازوکار اثبات کار حل می‌کند. بلاک‌ها فقط در صورتی از نظر همه اعضای شبکه معتبر هستند که اثبات کار آن‌ها - که در قالب یک هَش ارائه می‌شود، معتبر باشد. این موضوع نودهای غیرمتمرکز شبکه را قادر می‌سازد تا بدون نیاز به اعتماد به یکدیگر، بر روی اعتبار یک زنجیره بلاک مشخص به توافق برسند. اثبات کار یک بلاک نمایانگر این واقعیت است که برای تولید این بلاک هزینه شده است، و به خودی خود چیزی را اثبات نمی‌کند. منابعی که ماینرها باید برای تولید بلاک‌ها هزینه کنند، آن‌ها را از ساختن بلاک‌های نامعتبر یا خالی که موجب اسپم شدن شبکه می‌شود، باز می‌دارد. همچنین کسب کارمزد تراکنش‌ها و پاداش تولید بلاک، آن‌ها را ترغیب به ساخت بلاک‌های معتبر می‌کند.

(تلاش می‌کنیم به مرور زمان کلمات بیشتری به این فرهنگ اضافه و آن را کامل کنیم)

فرهنگ توصیفی اصطلاحات بیت کوین توسط مترجمین ناشناس و به سرپرستی الف.آزاد در حال گردآوری، و به صورت یک پروژه بلندمدت تعریف شده است. نظارت و بازبینی فنی این کار با همراهی [@mytechmix](https://mytechmix) انجام می پذیرد.

لغت نامه شرکت [ریور فایننشیال](#) به عنوان مرجع نسخه اول این فرهنگ مورد استفاده قرار گرفته است.

وبسایت منابع فارسی بیت کوین

پاییز ۱۴۰۰

bitcoind.me

منابع فارسی بیت کوین

معرفی کتابها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت کوین، اقتصاد، و حریم خصوصی که توسط علاقمندان و فعالان جامعه فارسی زبان بیت کوین تالیف یا ترجمه شده اند