

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، می‌توان سومی را محاسبه کرد. یک ویژگی قدرتمند امضاهای تطبیقی این است که یکی از طرفین معامله می‌تواند بر اساس یک داده محرمانه یک امضای تطبیقی ایجاد کند، و طرف مقابل نیز می‌تواند امضای تطبیقی خود را بر اساس همان داده‌ها تولید کند بدون اینکه نیاز باشد از داده‌های 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 نشده‌ای که ۱ بیت کوین به بابک ارسال می‌کند را به او می‌دهد. این تراکنش هنوز توسط آوا امضاء نشده است، بنابراین هنوز امکان منتشر شدن روی شبکه بیت کوین را ندارد، ولی به مقدار محرمانه‌ای که در آن وجود دارد پایبند است. در مرحله بعد، بابک تراکنشی ایجاد می‌کند که در آن ۱ بیت کوین به آوا ارسال می‌شود. بابک می‌تواند 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 می‌گذارد.

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 شده‌اش روی زنجیره بیت کوین، می‌تواند با استفاده از امضای تطبیقی و امضای اولیه خود، داده مخفی را محاسبه کند. با استفاده از این داده مخفی او می‌تواند امضای تراکنش آوا را بدست آورد. بابک اکنون می‌تواند 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 می‌شود و به صورت رشته‌ای از حروف و اعداد به نمایش در می‌آید. معمولاً مفهوم آدرس و کلید عمومی به جای یکدیگر بکار گرفته می‌شوند ولی آدرس در واقع هش یک کلید عمومی است. در حال حاضر برای دریافت بیت کوین از آدرس‌ها، و نه کلیدهای عمومی استفاده می‌شود. از نظر فنی یک آدرس علاوه بر هش کلید عمومی، اطلاعات بیشتری را در خود ذخیره می‌کند. کاربران می‌توانند توسط یک کیف پول بیت کوین به هر مقدار که نیاز داشته باشند، آدرس تولید کنند. کاربران کیف پول‌ها همچنین قادرند به آدرس‌های 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 هِش 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 کم 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 سایز تراکنش محاسبه می‌شود، ادغام چندین تراکنش در یک تراکنش واحد می‌تواند سایز 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.

گُذبندي بِش-۳۲

Bech32

روشی برای گُذبندي آدرس‌های سگويت 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 گُذبندي شامل مکانیزم تشخیص خطا است.

گُذبندي بِش-۱۳۲م

Bech32m

این روش گُذبندي 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 گُذگذاری آدرس‌های نسخه ۱ سگويت 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.

بیپ-۳۹ (کلمات بازیابی)

BIP39 (Mnemonic Phrases)

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

در حالی که استاندارد بیپ-۳۹ تقریباً توسط همه کیف پول‌های محبوب بیت کوین مورد پذیرش قرار گرفته است، اما همچنان در نرم‌افزار بیت کوین 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 بیت کوین استفاده کرد.

بیت

Bit

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 میلیونیم 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.

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. هر کس 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 هر کس می‌تواند کُد آن را تکثیر و به دلخواه خود ویرایش کند. اگر یک توسعه‌دهنده قصد دارد کُد 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 می کنند بخشی از هزینه های این افراد را از طریق کمک های مالی و کمک های 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 همه عملگرهای منطقی رایج در زبان‌های اسکریپت‌نویسی پشتیبانی نمی‌کند و باعث می‌شود اطمینان داشته باشیم که هیچ‌گونه اسکریپت 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 بیت‌کوین‌های قفل‌شده استفاده می‌شود، و برای ساخت اپلیکیشن‌ها و اجرای آن‌ها روی زنجیره بیت‌کوین مورد استفاده قرار نمی‌گیرد. سادگی اسکریپت، موجب افزایش امنیت بیت‌کوین می‌شود.

تمام تراکنش‌های بیت‌کوین برای تعریف روش باز شدن قفل بیت‌کوین‌هایی که روی یک خروجی تراکنش قرار دارند، از زبان اسکریپت استفاده می‌کنند. به عبارت دیگر، در یک تراکنش، این اسکریپت است که مشخص می‌کند بیت‌کوین ارسال شده متعلق به چه کسی است. بیت‌کوین دارای انواع اسکریپت‌های مختلف است ولی یکی از معروف‌ترین آن‌ها P2PKH است که درواقع آدرس‌هایی هستند که با عدد ۱ شروع می‌شوند. انواع دیگر اسکریپت می‌توانند قوانین پیچیده‌تری تولید کنند، مانند آدرس‌های چند امضایی. در این شرایط برای نقل و انتقال بیت‌کوینی 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 اسکریپت، اسکریپت‌های سگویی P2WPKH و P2WSH هستند که به کارگیری آن‌ها موجب صرفه‌جویی در کارمزد تراکنش خواهد شد.

Bitcoin Whitepaper

وایت‌پیپر بیت‌کوین

وایت‌پیپر یک مقاله علمی برای معرفی یک ایده جدید است، یا موضوعی را برای بحث مطرح می‌کند. وایت‌پیپر بیت‌کوین درواقع بیت‌کوین را به‌عنوان «سیستم پول نقد بر پایه یک سیستم همتا-به-همتا» معرفی می‌کند که «نیازی به اعتماد اشخاص ثالث ندارد». ساتوشی ناکاموتو وایت‌پیپر بیت‌کوین 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 است از تراکنش‌های معتبری 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 به‌طور میانگین حدود ۲,۰۰۰ تراکنش را در خود جای می‌دهند اما این تعداد ممکن است در آینده با پیشرفت‌های پروتکل بیت کوین افزایش یابد. با توجه به اینکه صرافی‌های بزرگ امروزه برای پرداخت‌های خود از ویژگی ارسال گروهی بیت کوین استفاده می‌کنند، نمی‌توان تعداد تراکنش‌های یک بلاک را به‌عنوان معیاری برای شمارش تعداد «پرداخت»‌های انجام شده در بلاک مورد نظر تعیین کرد و تعداد پرداخت‌ها می‌تواند ده‌ها برابر بیشتر از تعداد تراکنش‌ها باشد.

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 آبشاری به سمت جلو حرکت می‌کند و ارتباط همه بلاک‌هایی که پس از بلاک شماره ۴۰۰ آمده‌اند را از یکدیگر قطع می‌کند. این ویژگی تضمین می‌کند که پس از اضافه شدن یک بلاک به زنجیره بلاک‌های بیت‌کوین، دیگر نمی‌توان آن بلاک یا هریک از تراکنش‌های موجود در آن را تغییر داد.

بلاک اکسپلورر (کاوشگر بلاک)

Block Explorer

بلاک اکسپلورر سرویسی است که عموم افراد را قادر می‌سازد بلاک‌ها، آدرس‌ها، و تراکنش‌های زنجیره بیت‌کوین را مرور، و از وضعیت آن‌ها مطلع شوند. زنجیره بلاک‌های بیت‌کوین در دسترس عموم افراد قرار دارد. ده‌ها هزار نود در شبکه بیت‌کوین یک نسخه از زنجیره بلاک‌های بیت‌کوین را در خود ذخیره کرده‌اند و این موضوع صاحبان آن‌ها را قادر می‌سازد تا هریک از تراکنش‌ها و بلاک‌هایی که در شبکه بیت‌کوین منتشر می‌شود را دریافت کنند، اعتبار آن‌ها را بسنجند، و موجودی بیت‌کوین خود را محاسبه کنند. یک بلاک اکسپلورر این خدمات را برای افرادی که نود شخصی خود را اجرا نمی‌کنند فراهم می‌کند.

اما این سهولت به قیمت از بین رفتن حریم خصوصی و اعتماد به یک شخص ثالث تمام می‌شود. اغلب بلاک اکسپلوررها سرویس خود را در قالب یک وب‌سایت به کاربران ارائه می‌کنند و ممکن است داده‌های مربوط به آدرس IP کاربران، مکان فیزیکی، و آدرس‌های بیت‌کوین استعلام گرفته شده توسط کاربران سایت خود را جمع‌آوری کنند و این موضوع به شدت به حریم خصوصی کاربران این وب‌سایت‌ها لطمه می‌زند. برخی از بلاک اکسپلوررها برای حل این مشکل و حفظ حریم خصوصی، به کاربران خود اجازه می‌دهند که نرم‌افزار این سرویس را به صورت محلی و بر روی نود خود اجرا کنند.

برای امتحان یک بلاک اکسپلورر و خدماتی که ارائه می‌کند، از سایت mempool.space بازدید، و فهرست کامل بلاک‌های شبکه بیت‌کوین و تراکنش‌های آن‌ها را مرور کنید. پیشنهاد می‌شود برای

حفظ حریم خصوصی، آدرس‌ها و تراکنش‌های شخصی خود را وارد این سایت نکنید.

سربرگِ بلاک

Block Header

یک بلاک در زنجیرهٔ 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:

- شمارهٔ بلاک در طول زنجیره: عددی است که نشان می‌دهد قبل از بلاک موردنظر، چه تعداد بلاک وجود دارد.
- هشِ بلاک: نمایندهٔ عدد اثباتِ کار است.
- هشِ بلاک قبل: قرار گرفتن این مقدار در سربرگِ بلاک غیرقابل تغییر بودن بلاک‌های قبلی را تضمین می‌کند.
- برچسبِ زمان: نشان می‌دهد که بلاک موردنظر در چه زمانی منتشر شده است.
- ریشهٔ مرکب: هشِ همهٔ تراکنش‌هایی است که در بلاک موردنظر قرار گرفته است.
- سختی شبکه: این مقدار به روش خاصی گُذبنده 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 اثباتِ کار معتبری برای بلاک پیدا کنند.

سربرگِ بلاک نقش چکیدهٔ آن را ایفا می‌کند و با توجه به ساینز کوچکی که دارد می‌تواند سریع‌تر از خودِ بلاک بین نودهای شبکه منتقل و پردازش شود. ماینرها برای پیدا کردن عدد اثباتِ کارِ 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

ماینها مجبور بودند همه اطلاعات بلاک را برای پیدا کردن عدد اثبات کار هش کنند، در این صورت ممکن بود برای بالا بردن بهره‌وری خود، بلاک‌های خالی تولید کنند و این مسأله منجر به پایین آمدن ظرفیت پردازش تراکنش‌ها در شبکه بیت کوین می‌شد.

شماره بلاک در طول زنجیره

Block Height

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.

پاداش بلاک

Block Reward

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

Block Weight

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

Blockchain

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 دفتر کل 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 دفتر کل حسابداری را در خود ذخیره می‌کنند، بنابراین شبکه بیت کوین یک شبکه غیرمتمرکز است.

یکی از ویژگی‌های خاص یک زنجیره 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.

بی تی سی

BTC

نماد بیت کوین است. برای نمونه یک بیت کوین با نماد 1BTC نمایش داده می‌شود. یک بیت کوین به ۱۰۰,۰۰۰,۰۰۰ واحد کوچکتر به نام ساتوشی یا sats بخش پذیر است. یک ساتوشی در قراردادهای هوشمند شبکه لایتینگ -لایه بیرونی زنجیره اصلی بیت کوین،- به ۱,۰۰۰ واحد کوچکتر تقسیم می‌شود. بنابراین بیت کوین روی شبکه لایتینگ ۱,۰۰۰ برابر بخش پذیرتر از شبکه اصلی است. اگرچه باید این نکته را در نظر گرفت که واحد میلی ساتوشی روی زنجیره اصلی بیت کوین 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. داده تراکنش‌های بیت کوین، اسکرپت‌ها، کلیدهای عمومی، و بلاک‌ها مجموعه‌ای از بایت هستند که در قالب هگزادسیمال نمایش داده می‌شوند.

تاب آوری در برابر خطای بیزانس

Byzantine Fault Tolerance

تاب آوری 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 مسأله ژنرال‌های بیزانس را حل کرده و قادر است در مقابل حملات سیل ایستادگی کند.

در یک سیستم غیرمتمرکز که برای استفاده از آن نیاز به کسب مجوز نیست، هرکس می‌تواند به شبکه بپیوندد 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 بپیوندد 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.

مسأله ژنرال‌های بیزانس

Byzantine Generals Problem

این مسأله 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 مسأله 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.

بیت‌کوین مسئله 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 هش 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، بازمی‌دارد. همچنین کسب کارمزد تراکنش‌ها و پاداش تولید بلاک، آن‌ها را ترغیب به ساخت بلاک‌های معتبر می‌کند.

C

اثر کانتیلان

Cantillon Effect

اثر کانتیلان، اثر نابرابر تورم بر قیمت کالاها و دارایی افراد در اقتصاد را شرح می‌دهد. با توجه به اینکه پول‌های چاپ شده توسط بانک‌های مرکزی از طریق کانال‌های متفاوتی وارد اقتصاد می‌شوند، افراد و صنایع مختلف نیز اثرات آن را در برهه‌های زمانی مختلفی تجربه خواهند کرد. این موضوع در قیمت‌ها اعوجاج به وجود می‌آورد و به نفع برخی از خواص است، در حالی که برای برخی دیگر از گروه‌های جامعه اثرات خانمان‌براندازی دارد.

طبیعی است که پس از وارد شدن پول‌های چاپ شده جدید به اقتصاد، قیمت کالاها و دارایی‌ها افزایش یابند، با این حال قیمت همه اجناس به یکباره بالا نمی‌رود. اثر کانتیلان ادعا می‌کند اولین افرادی که این پول‌های جدید را دریافت می‌کنند، درواقع این فرصت را دارند که قبل از بالا رفتن قیمت‌ها، آن را خرج کنند.

این موضوع تا اندازه‌ای به این دلیل است که هزینه خلق پول فیات جدید که به گروه‌های خاص - معمولاً بانک‌ها - داده می‌شود، تقریباً صفر است. این بانک‌ها فرصت دارند تا این پول را برای به دست آوردن دارایی‌هایی که هنوز به دلیل افزایش پایه پولی گران‌تر نشده‌اند، صرف کنند. بنابراین می‌توان گفت بانک‌ها و افرادی که به وام‌های بانکی دسترسی دارند کالاها و دارایی‌ها را با تخفیف خریداری می‌کنند.

همین‌طور که این پول جدید از بانک‌های مرکزی به بانک‌های خصوصی، و از آنجا به سرمایه‌گزاران و در نهایت به دست مردم عادی می‌رسد، رشد پایه پولی اثر خود را بر قیمت‌ها می‌گذارد و قیمت‌ها نیز به تدریج افزایش می‌یابند. مردم عادی تاثیر رشد پایه پولی را زمانی تجربه می‌کنند که قیمت‌ها بالا رفته و آن‌ها اقلام مورد نیازشان را به قیمت بالاتری خریداری می‌کنند.

بنابراین، جریان وارد شدن پول‌های جدید به اقتصاد برای گروه‌هایی که آن را قبل از دیگران به دست می‌آورند سود بیشتری دارد و افرادی که آن را دیرتر دریافت می‌کنند، چندان سودی از آن نخواهند برد. بنابراین می‌توان ادعا کرد که مزایای مالی افراد و نهادهای نزدیک به بانک مرکزی - مثل بانک‌ها و صاحبان دارایی‌ها،- به قیمت زیان افرادی که ارتباطی با این نهادها ندارند، فراهم می‌شود.

می‌توان گفت تورم پدید آمده در نتیجه اثر کانتیلان در واقع مالیاتی بر قدرت خرید شهروندان است که به صورت غیرقانونی از سوی دولت‌ها تعیین، و به صورت غیرمستقیم از آن‌ها دریافت می‌شود.

پول نقد

Cash

پول نقد به دارایی گفته می‌شود که به عنوان واحد حساب و کتاب، ابزار پرداخت، و ذخیره ارزش استفاده شود. اما مهم‌تر از همه ویژگی‌های بالا پول نقد ابزار پرداختی است که در وجه حامل است، یعنی صاحب آن کسی است که آن را در اختیار دارد، بنابراین پس‌انداز آن هیچ گونه خطری برای دارنده آن ایجاد نمی‌کند.

این پول، نقدترین دارایی در یک اقتصاد است چون دارنده آن می‌تواند آن را به سرعت به هر چیزی که نیاز داشته باشد تبدیل کند. استفاده از پول فیات به عنوان ابزاری برای پرداخت، و واحد حساب و کتاب کارآمد است اما به دلیل عرضه نامحدود آن از سوی دولت‌ها، ابزار خوبی برای ذخیره ارزش نیست. امروزه بیت کوین نیز به عنوان ابزاری برای پرداخت استفاده می‌شود و با توجه به کمیابی و محدودیت عرضه آن -برخلاف پول فیات،- روش بسیار کارآمدی برای حفظ ارزش سرمایه کاربران آن است.

مقاوم در برابر سانسور

Censorship Resistance

بیت کوین به گونه‌ای طراحی شده که در برابر سانسور مقاوم باشد. این بدان معنا است که هیچ فرد یا نهادی نمی‌تواند یک کیف پول یا آدرس بیت کوین را به لیست سیاه وارد کند، زیرا هر نود قادر

است یک تراکنش را در شبکه بیت کوین منتشر کند و با توجه به کارکرد کارمزد تراکنش در ایجاد انگیزه اقتصادی لازم برای ماین شدن تراکنش‌ها توسط ماینرها، سانسور تراکنش‌های بیت کوین عملاً غیرممکن است.

هنگامی که یک تراکنش بیت کوین به شبکه ارسال می‌شود، بین نودهای شبکه دست‌به‌دست می‌شود تا زمانی که همه نودها آن را دریافت کنند. نودها همه تراکنش‌های تأیید نشده را در یک پایگاه داده به نام م‌پول نگهداری می‌کنند. ماینرها برای ساختن یک بلاک و اضافه کردن آن به زنجیره، از تراکنش‌های تأیید نشده موجود در م‌پول انتخاب می‌کنند. هنگامی که یک ماینر یک بلاک جدید می‌سازد، تراکنش‌های موجود در آن از م‌پول حذف، و به‌عنوان تراکنش‌های تأیید شده در نظر گرفته می‌شوند.

تا زمانی که افراد بتوانند به یکی از نودهای شبکه بیت کوین دسترسی پیدا کنند، خواهند توانست تراکنش خود را روی شبکه منتشر و اطمینان داشته باشند که این تراکنش با توجه به انگیزه اقتصادی که پیشتر به آن اشاره شد، تأیید خواهد شد. توسعه‌دهندگان بیت کوین به‌منظور جلوگیری از تلاش‌های دولت‌ها یا سایر نهادهای بزرگ برای سانسور تراکنش‌های کاربران بیت کوین، روش‌های منحصربه‌فردی برای انتشار و دست‌به‌دست شدن تراکنش‌ها بین نودها طراحی کرده‌اند. از جمله این روش‌ها می‌توان به راه‌کارهایی که شبکه‌های مش، ارتباطات ماهواره‌ای، یا رادیوهای آماتوری را به خدمت می‌گیرند اشاره کرد.

Chain Analysis

پایش زنجیره

پایش زنجیره، ترفندی برای تجزیه و تحلیل زنجیره بلاک بیت کوین و ردیابی دارایی افراد از طریق رصد تراکنش‌ها است. در این حوزه چند شرکت وجود دارند که کار آن‌ها فقط رصد تراکنش‌های افراد و شناسایی آن‌ها از راه به‌کارگیری این ترفندها است. این شرکت‌ها نتایج تجزیه و تحلیل خود را به مؤسسات مالی و دولت‌هایی که تلاش می‌کنند از کلاهبرداری، پول‌شویی، و سایر فعالیت‌های غیرقانونی جلوگیری کنند، می‌فروشند. پایش زنجیره یک مفهوم گسترده است و نباید با شرکت Chainalysis که در این حوزه فعالیت می‌کند اشتباه گرفته شود.

سیستم حسابداری بیت کوین برخلاف بانک‌ها بر پایه حساب مشتریان نیست. در عوض کاربران بیت کوین صاحب بخش‌هایی از بیت کوین هستند که خروجی خرج نشده نام دارد. این خروجی‌های خرج نشده شبیه به اسکناس هستند که اگر ارزش آن‌ها بیشتر از صورت حساب باشد صاحب آن‌ها یعنی فردی که بیت کوین ارسال کرده، مبلغی به عنوان باقی پول دریافت می‌کند. به عنوان مثال، اگر شما به فردی ۴ هزار تومان بدهکار باشید و قلکی داشته باشید که در ۵ هزار تومان باشد، باید آن را بشکنید، ۴ هزار تومان‌اش را به آن فرد بدهید و هزار تومان باقی را در یک قلمک جدید بگذارید.

یک کاربر برای ایجاد یک تراکنش بیت کوین، یکی از خروجی‌های خرج نشده خود را به عنوان ورودی انتخاب، و خروجی‌های لازم را نیز به آن اضافه می‌کند. یکی از این خروجی‌ها به آدرس گیرنده ارسال می‌شود و دیگری به عنوان باقی پول به کیف پول فرستنده و در قالب یک آدرس جدید باز می‌گردد. مقدار این خروجی درواقع حاصل تفریق ورودی و حسابی است که فرستنده بیت کوین با فرد دریافت کننده دارد.

فرض کنیم بابک به آوا ۴ بیت کوین بدهکار باشد و بخواهد این بدهی را تسویه کند. کیف پول او یک خروجی خرج نشده ۵ بیت کوینی دارد، بنابراین یک تراکنش با ورودی ۵ بیت کوین ساخته می‌شود، این تراکنش ۲ خروجی خواهد داشت، یکی ۴ بیت کوین به آوا ارسال می‌کند، و دومی ۱ بیت کوین به عنوان باقی پول به بابک بازمی‌گرداند. در عمل کارمزد تراکنش از خروجی دوم کسر می‌شود و درواقع مقداری که بابک پس می‌گیرد از ۱ بیت کوین کمتر خواهد بود.

یک جمع‌آزما رشته داده کوتاهی در قالب بایت است که به انتهای قطعه بزرگ‌تری از یک داده اضافه، و کار بررسی اعتبار آن را آسان می‌کند. با به کارگیری این روش می‌توان به آسانی از اشتباهات تایپی یا دستکاری داده‌ها جلوگیری کرد. جمع‌آزماها اغلب از چند بایت اول هش داده مورد نظر ساخته می‌شوند.

هنگامی که داده‌ای دارای یک جمع‌آزما باشد، هرکسی می‌تواند با بررسی آن اطمینان حاصل کند که

هش داده مورد نظر با این جمع آزمون مطابقت دارد و این داده از زمان ساخته شدن جمع آزمون تغییر نکرده است.

برای ساختن یک جمع آزمون در پروتکل بیت کوین تابع هش SHA-256 به صورت دو بار پشت سر هم مورد استفاده قرار می گیرد و جمع آزمایها در ساختن آدرس ها و کلیدهای خصوصی در الگوی WIF کاربرد دارند زیرا این داده ها بین کاربران و سرویس ها مبادله می شوند و ممکن است در حین انتقال بر اثر اشتباهات تایپی مخدوش شوند.

سی پی اف پی Child-Pays-for-Parent (CPFP)

سی پی اف پی یک تراند در مدیریت تراکنش های تأیید نشده بیت کوین است و هدفی مشابه با آربی اف را دنبال می کند. آربی اف این امکان را برای فرستنده بیت کوین فراهم می سازد تا با افزایش کارمزد، انگیزه ماینرها را برای تأیید تراکنش بالا ببرد و در نتیجه سرعت تأیید تراکنش ارسالی خود را افزایش دهد، در مقابل سی پی اف پی به گیرنده تراکنش این اجازه را می دهد تا از این راه زمان مورد نیاز برای تأیید تراکنش دریافت شده را کاهش دهد.

در موقعیتی که یک تراکنش با کارمزد پایین به شبکه ارسال شده باشد گیرنده می تواند برای تسریع در تأیید این تراکنش، تراکنش جدیدی را ایجاد کند که بیت کوین دریافتی را - با وجود اینکه هنوز تأیید نشده و در مم پول نودهای شبکه قرار دارد، - خرج می کند. تراکنش دوم کارمزد بالایی برای ماینرها در نظر می گیرد، بنابراین این انگیزه اقتصادی را برای آنها ایجاد می کند که اگر مایل به کسب این کارمزد بالا هستند، باید تراکنش قبلی را نیز در بلاک قرار دهند. در این صورت تراکنش اول دریافت کننده بیت کوین علیرغم کارمزد پایین، سریع تر تأیید خواهد شد.

گزینش کوین یعنی در زمان ایجاد یک تراکنش بیت کوین، یک یا چند عدد از خروجی‌های خرج‌نشده‌ای که کیف پول در اختیار دارد را خودمان به صورت دستی انتخاب کنیم. در هنگام ساخت یک تراکنش کیف پول‌های بیت کوین اغلب این وظیفه را بر اساس الگوهای از پیش تعیین شده و به صورت خودکار از جانب کاربران انجام می‌دهند و بسته به مقدار بیت کوینی که ارسال می‌شود، تعدادی از خروجی‌های خرج‌نشده را به عنوان ورودی تراکنش انتخاب می‌کنند.

به عنوان مثال، اگر آوا بخواهد به بابک ۱ بیت کوین بدهد و کیف پول او دارای خروجی‌های خرج‌نشده‌ای در مقادیر مختلف و در مجموع ۵ بیت کوین باشد، کیف پول او باید از میان خروجی‌های خرج‌نشده موجود یک یا تعدادی را به عنوان ورودی انتخاب کند. خروجی‌های خرج‌نشده‌ای که انتخاب می‌شوند به اولویت صاحب کیف پول بیت کوین بستگی دارند و این موضوع اساساً مقوله مهمی است. برخی از کیف پول‌ها انتخاب خروجی‌های خرج‌نشده با مقادیر بالا را در اولویت قرار می‌دهند تا با این کار از انباشت خروجی‌های خرج‌نشده داست جلوگیری کنند و همچنین کارمزد پایین‌تری برای آن پرداخت کنند. برخی دیگر از کیف پول‌ها برای حفظ حریم خصوصی کاربران خود خروجی‌های خرج‌نشده را به صورتی انتخاب می‌کنند که خروجی باقی پول در تراکنش وجود نداشته باشد.

گزینش کوین معمولاً توسط الگوریتمی که در کیف پول تعریف شده، انجام می‌شود، اما برخی از کیف پول‌ها به کاربران این اجازه را می‌دهند تا ترجیحات گزینش کوین خود را با توجه به نیازهای خود در بخش تنظیمات کیف پول تعیین کنند.

تراکنش کوین بیس اولین تراکنش هریک از بلاک‌های زنجیره بیت کوین است. ماینرها در این تراکنش به مقدار یارانه ساخت بلاک - که در حال حاضر ۶.۲۵ بیت کوین است، - و همچنین جمع کارمزد همه تراکنش‌هایی که در بلاک مورد نظر قرار دارند، بیت کوین دریافت می‌کنند.

این تراکنش تنها تراکنش موجود در بلاک است که ورودی ندارد ولی با توجه به اینکه بیت کوین‌های جدید از این طریق خلق می‌شوند، معتبر است. برای مشاهده یک تراکنش کوین بیس، اولین تراکنش یکی از بلاک‌های زنجیره بیت کوین را در یک کاوشگر بلاک ببینید.

کوین جویین

CoinJoin

کوین جویین یک تراکنش بیت کوین است با ورودی و خروجی‌های خاصی که آن را از دیگر تراکنش‌های شبکه بیت کوین متمایز می‌کند. ورودی‌های این تراکنش برخلاف اغلب تراکنش‌های بیت کوین متعلق به یک نفر نیست و همه خروجی‌های آن یک اندازه هستند. این ویژگی باعث می‌شود که تعیین صاحبان خروجی‌های این تراکنش برای یک ناظر بیرونی بسیار دشوار باشد. کوین جویین از راه بی‌اثر ساختن ترفندهایی که شرکت‌های پایش زنجیره بیت کوین به کار می‌بندند موجب حفظ حریم خصوصی کاربران بیت کوین می‌شود. یک تراکنش کوین جویین احتمال تشخیص مالکان کوین‌های ورودی را کاهش می‌دهد.

کوین جویین با سرویس‌های میکس از این لحاظ متفاوت است که برخلاف سرویس‌های میکس به صورت امانی اجرا نمی‌شود و برای کوین جویین نیازی به اعتماد به سرویس‌دهنده آن نیست. چرا که اختیار کوین‌ها از ابتدا تا انتهای فرآیند کوین جویین همواره در دستان صاحبان کوین‌ها است. می‌توانید نمونه‌ای از یک تراکنش کوین جویین شده را [در اینجا](#) ببینید. همانطور که مشاهده می‌کنید با توجه به یکسان بودن خروجی‌های این تراکنش، تعیین ارتباط میان خروجی‌ها و ورودی‌ها تقریباً غیرممکن است.

شرکت‌کنندگان در یک دور کوین جویین برای ساختن تراکنش و تأمین ورودی‌های آن با یکدیگر تعامل، و مجدداً کوین خود را در خروجی این تراکنش دریافت می‌کنند. همانطور که پیشتر اشاره شد، مقادیر همه خروجی‌های این تراکنش با یکدیگر برابرند.

کُلد استوریج به یک روش ذخیره سازی اطلاعات گفته می شود که در آن هیچ گونه ارتباطی با اینترنت یا دستگاه های دیگر وجود نداشته باشد. یک کیف پول کُلد استوریج شکلی از ذخیره سازی است و اغلب توسط بیت کوینرها برای نگهداری از بیت کوین هایی به کار می رود که معمولاً قرار نیست در فواصل زمانی کوتاه جابه جا شوند.

اگر یک کیف پول کلیدهای خصوصی را در حالت ایزوله و منفصل از اینترنت نگهداری کند، به آن کلد استوریج می گویند. با این حال، می توان کلیدهای عمومی این کیف پول کلد استوریج را در یک دستگاه جداگانه که به اینترنت متصل است وارد کرد. این روش به کاربران اجازه می دهد تا بیت کوین ها را به صورت مستقیم و بدون پایین آمدن امنیت روی کلد استوریج خود دریافت کنند.

روش نگهداری از بیت کوین روی کلد استوریج امن تر از کیف پول های متصل به اینترنت است، زیرا تقریباً تمام بدافزارها از طریق اینترنت به دستگاه ها نفوذ می کنند. با این حال، این روش در کنار امنیتی که با خود به همراه می آورد برای کاربران دشوار است. بنابراین، بهتر است از آن برای نگهداری مقادیر بالای بیت کوین که به طور روزمره مورد استفاده قرار نمی گیرد، استفاده شود.

ترفند مالک مشترک ورودی های یک

Common Input Ownership

تراکنش

Heuristic

یکی از مهم ترین ترفندهایی است توسط شرکت های تجزیه و تحلیل زنجیره بیت کوین، برای تشخیص هویت مالکان کوین های مورد نظر به کار گرفته می شود. در حال حاضر این ترفند فرض را بر این می گذارد که همه ورودی های یک تراکنش متعلق به یک نفر هستند.

این ترفند به هیچ وجه قطعی نیست، و با توسعه هرچه بیشتر بیت کوین غیر قابل اطمینان تر می شود. فن آوری هایی مانند کوین جوین، کوین سوپ، تراکنش های چندامضائی، و در آینده فن آوری هایی مثل MuSig که ادغام امضاهای کوین های ورودی را ممکن می سازد، هر چه بیشتر باعث بی اعتبار

شدن این ترفند خواهند شد.

تأییدیه تراکنش

Confirmation

وقتی یک تراکنش تأییدیه اول را دریافت می‌کند، این بدان معنی است که به داخل یکی از بلاک‌های زنجیره راه یافته است. هنگامی که این اتفاق می‌افتد، هر بلاک بعدی که به زنجیره بیت کوین اضافه شود، تأیید دیگری به این تراکنش اضافه می‌کند و تغییر آن را به‌طور فزاینده‌ای دشوارتر می‌کند. معمولاً، هر تراکنش پس از دریافت ۶ تأییدیه، نهایی در نظر گرفته می‌شود.

یک تراکنش پس از منتشر شدن روی شبکه بیت کوین، بلافاصله تصفیه نمی‌شود بلکه ابتدا از طریق نودهای شبکه دست به دست، و به مempool آن‌ها اضافه می‌شود. این تراکنش در این مرحله در وضعیت «در انتظار تأیید» قرار دارد. ماینرها برای ساختن بلاک‌ها، پرسودترین تراکنش‌ها را -نسبت به فضایی که اشغال می‌کنند- انتخاب، و درون بلاک‌ها قرار می‌دهند. هنگامی که یک تراکنش درون یک بلاک قرار می‌گیرد، از mempool حذف، و وضعیت آن به «تأیید شده» تغییر می‌کند.

با این حال باید توجه کرد که این تراکنش پس از وارد شدن به یک بلاک در زنجیره، فقط یک تأیید دارد. به‌طور کلی پیشنهاد می‌شود تا زمانی که یک تراکنش ۶ تأییدیه دریافت نکرده، نهایی در نظر گرفته نشود. اگر یک تراکنش فقط ۱ تأییدیه داشته باشد، این امکان -هرچند بسیار کم- وجود دارد که بلاکی که این تراکنش مورد نظر در آن قرار دارد، به یک بلاک سرگردان تبدیل شود. در این مورد نادر، تراکنش مجدداً به mempool بازگردانده می‌شود و وضعیت آن بار دیگر از «تأیید شده» به «در انتظار» تغییر پیدا می‌کند. پذیرفتن تراکنش‌هایی که همچنان در انتظار تأیید هستند به‌هیچ‌عنوان توصیه نمی‌شود، زیرا ممکن است این تراکنش با یک تراکنش دیگر که کارمزد تراکنش بیشتری به ماینرها پرداخت می‌کند جایگزین، و بیت کوین‌ها به یک آدرس دیگر منتقل شوند.

اجماع وضعیت مطلوب در یک سیستم غیرمتمرکز مانند بیت کوین یا سایر پروژه‌های اپن سورس و به معنی توافق میان افراد حاضر در چنین شبکه‌هایی است. اجماع با دموکراسی متفاوت است؛ در سیستمی که بر پایه اجماع بنا شده رأی‌گیری، نمایندگی، اعتبارنامه، یا متولی‌گری وجود ندارد. رسیدن به اجماع مشروط به توافق میان همه اعضا نیست و از آنجا که همه طرف‌های درگیر اغلب با یکدیگر توافق مطلق ندارند، رسیدن به اجماع وضعیت مطلوب است.

اجماع در دو سطح متفاوت در بیت کوین مطرح است؛ اول، توافق در توسعه و نگهداری از سورس بیت کوین، دوم بین همه نودهای موجود در شبکه که به ذخیره‌سازی و اعتبارسنجی زنجیره بیت کوین مشغول‌اند. در سطح سورس نرم‌افزار، هر کس قادر است پیشنهادهای خود را مبنی بر اعمال تغییر یا توسعه سورس نرم‌افزار ارائه کند، و همچنین حق دارد در مورد پیشنهادهای دیگران نظر دهد و آن‌ها را آزادانه نقد کند. این روش باعث می‌شود فرآیند توسعه پروژه بیت کوین از دیگر پروژه‌های متمرکز کندتر باشد، زیرا قبل از اعمال هرگونه تغییر در سورس نرم‌افزار یا قوانین پروتکل، نیازمند بحث و بررسی و آزمون‌های دقیق و طولانی است. با این حال این فرآیند تضمین می‌کند که سلايق یک گروه برگزیده بر دیگران تحمیل نمی‌شود و هیچ فرد یا گروهی قادر به تغییر بیت کوین برای رسیدن به منافع خود نخواهد بود.

برای رسیدن به اجماع در سطح زنجیره بیت کوین، می‌بایست نرم‌افزار همه نودهای شبکه با یکدیگر سازگار باشند. همه نودهای موجود در شبکه باید بر روی پارامترهای اصلی پروتکل با یکدیگر توافق داشته باشند؛ قوانینی چون تعداد کوین‌هایی که به ازای هر بلاک تولید می‌شوند، و اینکه چه تراکنش‌ها و بلاک‌هایی معتبر هستند. این نودها علاوه بر این باید روی وضعیت دقیق زنجیره با یکدیگر توافق داشته باشند؛ مواردی چون توافق بر روی زنجیره اصلی بیت کوین و تراکنش‌های معتبری که در خود دارند. اگر نودها بر روی این پارامترها اختلاف داشته باشند، شبکه دچار گسست، و زنجیره بیت کوین چند پاره می‌شود. برقراری صلح میان زنجیره‌های مختلف که هر کدام از قوانین متفاوتی پیروی می‌کنند کار بسیار دشواری است. این موضوع نشان می‌دهد که حفظ توافق میان نودهای شبکه تا چه حد اهمیت دارد.

رمزنگاری یک رشته مطالعاتی بسیار گسترده و متنوع است. مطالعه الگوریتم‌های هَش، رمزگزاری و رمزگشایی، کلیدهای عمومی و خصوصی، همه در حوزه رمزنگاری قرار می‌گیرند. هر سه این مفاهیم اساساً مبتنی بر ریاضیات و احتمالات هستند. بیت کوین برای خلق یک دفتر کل غیرقابل تغییر، و یک سیستم غیرمتمرکز که برای استفاده از آن نیاز به اعتماد و کسب اجازه از هیچ نهاد یا شخصی نیست، از رمزنگاری استفاده می‌کند.

بیت کوین با استفاده از رمزنگاری بر پایه کلید عمومی کاربران را قادر می‌سازد کلیدهای خصوصی و عمومی خود را بسازند و بدون نیاز به اعتماد و کسب اجازه از هیچ شخص یا نهادی به دریافت و ارسال بیت کوین اقدام کنند. اینکه عنوان می‌شود استفاده از بیت کوین نیاز به کسب مجوز ندارد، بدان معنی است که کاربران برای استفاده از بیت کوین نیاز به اخذ تأییدیه از هیچ واسطه یا شخص ثالثی ندارند و می‌توانند مستقیماً آن را به کار بگیرند و اساساً تمایز بیت کوین با سیستم‌های بانکداری سنتی همین است.

علاوه بر این هنگامی که یک کاربر به منظور دریافت بیت کوین کلید عمومی خود را به کاربر دیگری ارسال می‌کند، اطمینان دارد که دریافت کننده کلید عمومی به هیچ عنوان قادر به سرقت بیت کوین‌های وی نخواهد بود. این اساساً با سیستم‌های مالی سنتی متفاوت است، چون در این سیستم‌ها به محض اینکه فردی اطلاعات کارت اعتباری خود را به یک فروشگاه دهد یا روی دستگاه کارت‌خوان فروشگاه کارت بکشد درواقع به آن‌ها اجازه کنترل حساب خود را داده است. البته بیشتر فروشندگان و فروشگاه‌های آنلاین تقلب نمی‌کنند و از حساب مشتریان خود اضافه برداشت نمی‌کنند ولی دلیل اصلی آن این است که کاربران برای پس گرفتن حق خود به دولت یا بانک‌ها اعتماد می‌کنند. اما در بیت کوین با توجه به به کارگیری روش رمزنگاری با کلید عمومی، نیازی به اعتماد به هیچ فرد یا نهاد متمرکزی نیست.

یک کیف پول یا خدماتی که در آن کاربران مسئول کلید خصوصی خود نباشند، امانی است.

به عنوان مثال اغلب صرافی‌ها و کارگزاران امانی هستند زیرا کلید خصوصی کاربران تحت کنترل آنها است و این نهادها موجودی حساب کاربران را صرفاً بر اساس سیستم حسابداری داخلی خود به آنان نمایش می‌دهند.

ممکن است کیف پول‌های امانی امنیت بسیار بالایی داشته باشند، اما فعالیت آنها در چهارچوب قوانین دولتی است و از طرف دیگر راهی برای ممیزی آنها نیز وجود ندارد. توانایی ایفای تعهدات یا راستی‌آزمایی رعایت شیوه‌نامه‌های امنیتی یک شرکت سرویس‌دهنده امانی نمی‌تواند توسط یک کاربر معمولی مورد بررسی قرار گیرد. به همین ترتیب، اگر یک کاربر قصد دریافت بیت کوین روی یک بستر امانی را داشته باشد، باید خطر سانسور، یا مصادره شدن حساب خود را در نظر بگیرد. به همین دلیل معمولاً جامعه بیت کوین یکدیگر را به استفاده از روش‌های غیرامانی و در اختیار گرفتن کنترل کلیدهای خصوصی تشویق می‌کنند.

سایفرپانک

Cypherpunk

سایفرپانک عنوان یک گروه غیررسمی از افرادی است که به منظور حفاظت از حریم خصوصی و استقلال فردی، روی توسعه و خلق نرم‌افزار و سخت‌افزار تمرکز دارند. سایفرپانک‌ها نگران رقابت دولت‌ها برای ایجاد حکومتی بر پایه رصد و نظارت رفتار شهروندان، و همچنین سلطه شرکت‌های بزرگ بر فناوری و مالکیت معنوی هستند. ساتوشی ناکاموتو، خالق ناشناس بیت کوین و تقریباً تمام توسعه‌دهندگان اولیه بیت کوین مانند هل فینی سایفرپانک بوده‌اند.

همانطور که در بیانیه سایفرپانک آمده، آنها معتقدند دستیابی به آزادی و حفظ حریم خصوصی تنها از راه استفاده از رمزنگاری و نرم‌افزار امکان‌پذیر است و اعتقادی به فعالیت و لابی‌گری سیاسی ندارند. این موضوع به‌طور خلاصه در شعار آنها اینگونه بیان می‌شود: «سایفرپانک‌ها کُد می‌نویسند».

D

کاهش ارزش

Debasement

به کاهش عمدی ارزش پول می‌گویند. ارزش پول کالاهایی مانند سکه‌های طلا یا نقره از راه کاهش مقدار طلا یا نقره‌ای که در آن‌ها وجود دارد انجام می‌شود. برای کاهش ارزش اسکناس‌ها یا پول‌های ملی دیجیتال که تحت کنترل بانک‌های مرکزی قرار دارند، فقط کفایت مقدار بیشتری از آن‌ها خلق شود. این فرآیند معمولاً توسط دولت‌ها و به قصد تأمین هزینه فعالیت‌های آن‌ها از جیب شهروندان انجام می‌شود.

کاهش ارزش پول شهروندان راهی جایگزین برای دریافت مالیات مستقیم از آنهاست اما برخلاف مالیات که اثر خود را به صورت آنی روی زندگی افراد نشان می‌دهد، بیشتر مردم شناخت درستی از این روش جایگزین ندارند. به همین دلیل، دولت‌های مختلف از امپراتوری روم گرفته تا دولت ایالات متحده آمریکا برای کاهش ارزش پول خود از این روش استفاده کرده‌اند. برای نمونه دولت ایالات متحده در سال ۱۹۶۵ مقدار نقره موجود در سکه نیم دلاری را از ۹۰ به ۶۰ درصد کاهش داد، درحالی که بر اساس قانون هر دو سکه ارزش دلاری یکسانی داشتند.

دفتر کل حسابداری غیرمتمرکز

Decentralized Ledger

به آرشیو همه تراکنش‌های انجام گرفته روی یک شبکه که به صورت غیرمتمرکز نگهداری شود، دفتر کل حسابداری غیرمتمرکز می‌گویند. این دفتر کل با همکاری بسیاری از نودهای مستقل حاضر در شبکه، و بر اساس مجموعه قوانین پذیرفته شده میان آنان به روز و از آن حفاظت می‌شود. بیت کوین برای سازماندهی شبکه و حفاظت از دفتر کل حسابداری خود، از زنجیره بلاک و ساز و کار اثبات کار استفاده می‌کند.

بانک‌ها و سیستم‌های مالی سنتی برای نگهداری از اطلاعات حساب مشتریان خود از دفاتر کل

متمرکز استفاده می کنند. شعب بانک دفتر کل مرکزی را به صورت دوره ای به روز می کنند، اما این دفتر عمومی نیست و افراد عادی نیز قادر به حسابرسی آن نیستند. پروتکل بیت کوین این پارادایم را تغییر، و به همه افراد اجازه دسترسی مستقیم به دفتر کل را می دهد. هرکس می تواند یک تراکنش بیت کوین را در شبکه منتشر کند، سپس ماینرها این تراکنش را به زنجیره بلاک اضافه می کنند و با توجه به عمومی بودن زنجیره بلاک در شبکه بیت کوین همه می توانند برای بررسی موجودی و تاریخچه تراکنش های خود به آن رجوع کنند.

همه نودهای شبکه یک نسخه از دفتر کل حسابداری بیت کوین را در خود ذخیره می کنند تا امکان هیچ گونه تقلب در آن وجود نداشته باشد. این روش غیرمتمرکز موجب می شود تا این شبکه پاشنه آشیل نداشته باشد، این بدان معناست که سرور مرکزی وجود ندارد تا با خاموش کردن آن بتوان کل سیستم را از کار انداخت. همچنین راهی برای ایجاد دخل و تصرف در دفتر کل حسابداری وجود ندارد زیرا دفتر کل حسابداری بیت کوین عمومی و غیرمتمرکز است. شرایط در سیستم مالی و بانک های سنتی متفاوت است زیرا مدیران این سیستم ها قادرند خودسرانه اطلاعات موجود در دفتر کل حسابداری متمرکز تحت کنترل خود را تغییر دهند و کاربران این سیستم ها راهی برای حسابرسی و بازبینی دفتر کل متمرکز مورد استفاده را ندارند.

Denial of Service (DoS) Attack

حمله محروم سازی از سرویس

یک نوع حمله دیجیتال به یک سیستم یا یک فرد است که تلاش می کند قربانی را از یک شبکه حذف، و مانع دسترسی دیگران به او شود. این حمله معمولاً با به کارگیری از اسپم باعث هدر رفتن منابع قربانی، و توقف خدمات رسانی او به کاربران خواهد شد.

اگر این حمله اگر توسط گروهی از کامپیوترها و به صورت توزیع شده انجام شود، مقابله با آن اغلب دشوارتر خواهد شد زیرا نمی توان صرفاً با مسدود کردن یکی از حمله کنندگان آن را متوقف کرد.

در شبکه های همتا-به-همتا و عمومی مانند بیت کوین، مقابله با این نوع حملات یک موضوع چندوجهی است و باید با احتیاط بیشتری انجام شود زیرا در این شبکه ها اغلب گزینه های کمتری

برای قطع دسترسی بازیگران مخرب به شبکه وجود دارد.

مسیر استخراج کلید

Derivation Path

داده‌ای است که کیف پول‌های سلسله‌مراتبی قطعی از آن برای استخراج یک کلید مورد نظر از میان کلیدهای موجود در درخت کلیدها استفاده می‌کنند. استاندارد مسیرهای استخراج به همراه کیف پول‌های سلسله‌مراتبی قطعی تدوین و به‌عنوان بخشی از پیشنهاد توسعه و بهبود بیت کوین و با شماره ۳۲ معرفی شد.

سختی شبکه

Difficulty

سختی شبکه معیاری برای اندازه‌گیری دشواری ساختن یک بلاک در شبکه بیت کوین است. ماینرها برای ایجاد یک بلاک باید اثبات کار مربوطه را نیز در قالب یک هش به شبکه ارائه کنند. این هش درواقع عدد بزرگی است که باید از یک عدد مشخص کمتر باشد، در غیر اینصورت از نظر شبکه معتبر نیست. این عدد مشخص توسط قوانین پروتکل بیت کوین تعیین می‌شود.

سختی شبکه یک پارامتر ثابت نیست و هر ۲۰۱۶ بلاک -تقریباً هر دو هفته-، به‌روز می‌شود تا آهنگ تولید بلاک‌ها در شبکه ثابت باشد و ساخت هر بلاک تقریباً ۱۰ دقیقه طول بکشد. اگر ماینرهای بیشتری به شبکه اضافه شوند و بلاک‌های بیشتری در واحد زمان تولید شود، سختی شبکه افزایش می‌یابد. برعکس، اگر ماینرها دستگاه‌های خود را خاموش کنند و توان هش شبکه کاهش یابد، سختی شبکه کاهش می‌یابد. سختی شبکه معیاری است که به‌طور مستقیم به توان هش شبکه مرتبط است.

این عدد از یکی از داده‌های گُذبنده شده در سربرگ بلاک به نام «بیت» قابل استخراج است. این به نودهای شبکه این اجازه را می‌دهد تا درستی عدد اثبات کار را بررسی، و اعتبار بلاک مورد نظر را مورد بازبینی قرار دهند.

به الگوی خاصی از تراکنش‌های بیت‌کوین گفته می‌شود که برای اجرای یک قرارداد هوشمند سرویس‌های مرجعی مانند اوراکل‌ها را به کار می‌گیرند. می‌توان از طریق به کارگیری دی‌ال‌سی‌ها با استفاده از زنجیره بیت‌کوین قراردادهایی را به قصد شرط‌بندی ایجاد کرد. برای ساخت یک دی‌ال‌سی دو طرف مقداری بیت‌کوین روی یک آدرس چندامضایی قفل می‌کنند. برای آزاد کردن موجودی این قرارداد به اطلاعات خاصی که یک اوراکل در یک زمان خاص منتشر می‌کند، نیاز خواهد بود. اطلاعاتی که یک وب‌سایت در خصوص نتایج مسابقات ورزشی منتشر می‌کند، یا فهرست ارزش لحظه‌ای دارایی‌های مختلفی که در وب‌سایت صرافی‌ها قرار دارد هر کدام می‌توانند به عنوان یک اوراکل برای دی‌ال‌سی‌ها به کار گرفته شوند.

این نوع قراردادها به سایر قراردادهای هوشمند برتری دارند زیرا از دید زنجیره بلاک چیزی بیشتر از یک تراکنش چند امضایی نیستند. بدین ترتیب برای اجرای آن‌ها فقط به امضاهای شnor - که در ارتقاء پروتکل تپروت به قوانین شبکه اضافه خواهد شد، - نیاز است و برای به کار بستن آن‌ها لازم نیست تغییری در سطح پروتکل بیت‌کوین انجام پذیرد. با این حال، باید توجه داشت که قراردادهای دی‌ال‌سی قادر نیستند مشکل اعتماد به اوراکل‌ها را کاملاً حل کنند.

قضیه لگاریتم گسسته (دی‌ال‌پی)

Discrete Log Problem (DLP)

قضیه لگاریتم گسسته این موضوع را شرح می‌دهد که در حال حاضر هیچ روش شناخته شده‌ای برای محاسبه نتیجه عملگر تقسیم برای نقاطی که بر روی یک منحنی بیضوی قرار دارند، وجود ندارد. محاسبه نتایج عملگر ضرب که برای به دست آوردن کلیدهای عمومی از کلیدهای خصوصی مورد استفاده قرار می‌گیرد، به سادگی انجام می‌شود اما معکوس آن ممکن نیست.

این ویژگی منحصر به فرد امنیت رمزنگاری منحنی بیضوی را تضمین می‌کند. با این حال باید به این نکته توجه کرد که ناممکن بودن قضیه لگاریتم گسسته هنوز اثبات نشده است. بلکه می‌توان گفت که ریاضی‌دانان پس از انجام تحقیقات زیاد به این نتیجه رسیده‌اند که در حال حاضر راهی وجود

ندارد و متخصصان علم رمزنگاری بر همین اساس امنیت آن را پذیرفته‌اند.

امنیت بیت کوین نیز بر پایه قضیه لگاریتم گسسته تأمین می‌شود. بیت کوین برای پیاده‌سازی رمزنگاری کلید عمومی از منحنی بیضوی secp256k1 استفاده می‌کند. کلیدهای خصوصی اعداد تصادفی بزرگی هستند. برای به‌دست آوردن کلید عمومی P روی منحنی بیضوی، کلید خصوصی sk در یک عدد ثابت معلوم ضرب می‌شود. با توجه به قضیه لگاریتم گسسته امکان محاسبه معکوس عملگر ضرب وجود ندارد، بنابراین با معلوم بودن کلید عمومی، نمی‌توان کلید خصوصی را محاسبه کرد.

این ویژگی در سیستم‌های ECDSA و Schnorr برای ساختن امضاء دیجیتال به خدمت گرفته می‌شود. با استفاده از امضاء دیجیتال می‌توان بدون نیاز به فاش کردن کلید خصوصی ثابت کرد که تولیدکننده امضای دیجیتال کلید خصوصی مورد نظر را در اختیار دارد.

بخش پذیری

Divisibility

بخش‌پذیری یک ویژگی برای کالاها و اجناسی است که می‌توانند بدون از دست دادن ارزش‌شان به بخش‌های کوچک‌تری تقسیم شوند. از آنجا که حجم معاملات اقتصادی همواره متفاوت است، یک پول برای اینکه بتواند در اقتصاد به‌طور گسترده‌ای مورد استفاده قرار گیرد باید به اندازه کافی بخش‌پذیر باشد. همچنین ارزش یک پول نباید پس از تقسیم شدن به واحدهای کوچک‌تر کاهش پیدا کند.

بخش‌پذیری به واحدهای کوچک‌تر نقطه ضعف طلا به عنوان یک پول است، زیرا نمی‌توان آن را به راحتی به مقادیر کوچک‌تر تقسیم کرد. به منظور استفاده کارآمد از پول‌های ملی تحت کنترل بانک‌های مرکزی، این پول‌ها در واحدهای مختلف و به شکل اسکناس و سکه تولید می‌شوند.

بیت کوین به عنوان یک دارایی کاملاً دیجیتال از بخش‌پذیری بسیار بالایی برخوردار است. روی زنجیره بلاک بیت کوین می‌توان هر بیت کوین را به ۱۰۰ میلیون واحد کوچک‌تر به نام ساتوشی

تقسیم کرد. با این حال نقل و انتقال یک ساتوشی به دلایل مختلف از جمله کارمزد همیشه به صرفه نیست. شبکه لایتنینگ به عنوان یک لایه بیرونی روی زنجیره اصلی بیت کوین برای مدیریت حساب کاربران خود بخش پذیری هر بیت کوین را با تقسیم کردن هر ساتوشی به ۱۰۰,۰۰۰ واحد کوچکتر بیشتر می کند، اما باید توجه داشت که واحد میلی ساتوشی روی زنجیره اصلی بیت کوین تعریف نشده است.

یک پول را دوبار خرج کردن

Double Spend

به شرایطی گفته می شود که در آن فردی بتواند پولش را دوبار خرج کند و یک یا چند نفر را فریب دهد تا باور کنند واقعاً پولی دریافت کرده اند.

اقلام دیجیتالی مانند فایل های متنی و موسیقی را می توان به آسانی تکثیر کرد، اما قابلیت تکثیر شدن ویژگی مطلوبی برای یک پول نیست. مسئله دوبار خرج کردن یک پول به همین موضوع اشاره می کند: گیرنده یک پول دیجیتال از کجا اطمینان پیدا کند پولی که دریافت کرده به طور همزمان به فرد دیگری نیز فرستاده نشده است؟ اعضای یک شبکه پولی از کجا مطمئن باشند که دیگران پول هایشان را عمداً دوبار خرج نمی کنند؟

این مسأله در شبکه بیت کوین از طریق استفاده از یک دفتر کل حسابداری غیرمتمرکز که همه کاربران به آن دسترسی دارند، حل شده است. هنگامی که یکی از کاربران این شبکه بیت کوین خود را به فرد دیگری ارسال می کند، درواقع کوین ارسال شده از بین رفته و در قالب یک کوین جدید در اختیار فرد دریافت کننده قرار می گیرد. حذف این کوین در دفتر کل حسابداری بیت کوین که در دسترس همه کاربران است ثبت می شود تا صاحب قبلی قادر به ارسال مجدد آن به یک فرد دیگر نباشد.

داست

Dust

اگر مقدار یکی از خروجی های خرج نشده (کوین) به قدری کوچک باشد که پرداخت کارمزد

تراکنش در هنگام خرج شدن آن به صرفه نباشد، به آن داست گفته می‌شود. با افزایش کارمزد تراکنش در شبکه، کوین‌های بیشتری تبدیل به داست خواهند شد. برای جلوگیری از تبدیل خروجی‌های خرج نشده به داست بهتر است در مواقعی که مم پول خلوت و کارمزد تراکنش پایین است، کوین‌های کوچک را با یکدیگر ترکیب و به یک کوین بزرگ‌تر تبدیل کرد.

حمله داست

Dust Attack

گاهی اوقات یک مهاجم مقدار بسیار کمی بیت کوین -حدود ۵۰۰ ساتوشی،- به یک آدرس تصادفی ارسال می‌کند. اگر صاحب این کیف پول متوجه این موضوع نشود و این داست دریافت شده را در یکی از تراکنش‌های خود به عنوان یک ورودی وارد کند، در این صورت خطر نشت اطلاعات مالی خصوصی او به فرد مهاجم بسیار محتمل است.

یک حمله داست شبیه به اتصال یک دستگاه ردیاب به قربانی است، با این تفاوت که در این جا مهاجم به جای ردگیری مکانی قربانی، از اطلاعات مالی خصوصی و میزان دارایی او اطلاع پیدا می‌کند.

اگر به طور ناخواسته مقداری بیت کوین به حساب شما واریز شد، شما نباید آن را در کنار کوین‌های دیگر موجود در کیف پول خود به عنوان ورودی یک تراکنش وارد کنید. یک حمله داست در صورتی موفق خواهد بود که دریافت کننده داست، آن را در تراکنشی که شامل کوین‌های دیگر او می‌شود وارد کند.

E

ای سی دی اس ای

ECDSA

الگوریتم امضاء دیجیتال روی منحنی بیضوی یا ECDSA الگویی برای تولید امضاء دیجیتال با استفاده از کلید عمومی و خصوصی است. تمام کلیدها و امضاهای بیت کوین در حال حاضر از این روش تولید می‌شوند.

یک امضاء ECDSA به کاربران این امکان را می‌دهد تا امضاء دیجیتالی که با استفاده از کلید خصوصی ساخته و به همراه کلید عمومی منتشر شده است را بررسی و اطمینان حاصل کنند که این امضاء توسط صاحب کلید عمومی ایجاد شده است. استخراج کلید خصوصی از امضاء و یا کلید عمومی منتشر شده ممکن نیست. همچنین راهی برای جعل امضاء و استفاده از آن برای یک داده متفاوت وجود ندارد. با توجه به این ویژگی‌های امنیتی امضاء دیجیتال ECDSA در تراکنش‌های بیت کوین به کار گرفته شده است.

برای ساختن کلید عمومی، یک کاربر ابتدا باید یک کلید خصوصی تولید کند که در واقع چیزی جز یک عدد بزرگ نیست. سپس این کلید خصوصی باید در مختصات یک نقطه تعریف شده به نام نقطه مولد ضرب شود تا کلید عمومی به دست آید. این عملگر ضرب که در اینجا مطرح می‌شود، عملگر ضرب نقطه‌ای است و با عملگر ضرب معمولی تفاوت دارد. اساساً اعمال عملگر تقسیم بر روی منحنی بیضوی غیرممکن است، این بدان معنی است که در حال حاضر نمی‌توان کلید خصوصی را از روی کلید عمومی به دست آورد.

حمله خسوف

Eclipse Attack

این حمله روشی برای هدف قرار دادن یک نود خاص در شبکه از راه دوره کردن، و در نتیجه مخدوش نمودن برداشتی که این نود مورد نظر از وضعیت کل شبکه دارد است. به عنوان مثال، اگر

یک نود بیت کوین با ۸ نود دیگر در ارتباط باشد و همه آن ۸ نود در اختیار یک فرد مهاجم باشد، در این صورت این فرد قادر خواهد بود تا بلاک‌های جدیدی که ماینرها می‌سازند را به دست این نود نرساند. با وجود اینکه بقیه شبکه همچنان به کار پردازش و دست‌به‌دست کردن بلاک‌ها مشغول است، نود قربانی اطلاعاتی از آن‌ها پیدا نخواهد کرد.

اگر اجرای این حمله موفقیت‌آمیز باشد، مهاجم قادر است سوءاستفاده‌های مختلفی از قربانی کند. با این حال شبکه بیت کوین به گونه‌ای طراحی شده تا آسیب‌پذیری کمتری در مقابل چنین حمله‌ای داشته باشد. نودهای بیت کوین محدودیتی برای برقراری ارتباط با نودهای دیگر در شبکه غیرمتمرکز بیت کوین ندارند.

کدبندی^۸

Encoding

پروتکل بیت کوین برای نمایش اطلاعات از روش‌های کدبندی مختلفی استفاده می‌کند. این روش‌ها بسته به نوع داده مورد نظر و به‌منظور خوانایی هرچه بیشتر و صرفه‌جویی در فضای موردنیاز روی دیسک انتخاب می‌شوند. هرچه تعداد کاراکترهای به کار گرفته شده در یک روش کدبندی بیشتر باشد، داده خروجی متراکم‌تر و کوتاه‌تر خواهد بود. با این حال، برخی از کاراکترها مانند عدد صفر و حرف 0 با توجه به شباهت‌هایی که در برخی از فونت‌ها با یکدیگر دارند، قابلیت خوانایی پایینی دارند و در برخی از روش‌های کدبندی مورد استفاده قرار نمی‌گیرند. رایج‌ترین روش‌های کدبندی که بیت کوین از آن‌ها استفاده می‌کند به قرار زیر است:

هگزادسیمال: روشی برای کدبندی داده‌ها است که از ۱۶ کاراکتر یعنی ارقام ۰ تا ۹ و حروف a تا f استفاده می‌کند. بزرگ یا کوچک نوشتن حروف در این روش کدبندی تفاوتی ندارد و داده‌هایی که با این روش کدبندی شده‌اند اغلب با پیشوند 0x آغاز می‌شوند. کلیدهای عمومی، هَش‌ها، اسکرپیت‌ها و تراکنش‌ها معمولاً با الگوی هگزادسیمال کدبندی می‌شوند.

بیس-۵۸: این روش کدبندی از ۵۸ کاراکتر، شامل حروف کوچک و بزرگ الفبا و ارقام ۱ تا ۹ تشکیل شده است اما برای بالا بردن قابلیت خوانایی عدد صفر، حرف 0 بزرگ، حرف I بزرگ، و

حرف l کوچک در آن مورد استفاده قرار نمی‌گیرد. یکی از گونه‌های این روش کُدبندی روش بیس-۵۸ با قابلیت جمع‌آزمایی است که برای نمایش آدرس‌های قدیمی و کلیدهای خصوصی بیت‌کوین از آن استفاده می‌شود. یکی از اشکالات موجود در این روش کُدبندی، نبود سازوکاری برای ردیابی خطا است.

بیس-۶۴: این روش کدبندی شامل مجموعه‌ای ۶۴ کاراکتری است که از تمام حروف کوچک و بزرگ، ارقام صفر تا ۹، و همچنین دو کاراکتر + و / تشکیل شده است. تراکنش‌هایی که به صورت ناقص امضاء شده‌اند از این روش کدبندی می‌شوند.

بیش-۳۲: این روش تنها از حروف کوچک و اعداد استفاده می‌کند و عدد ۱، حروف i، b، و o برای افزایش قابلیت خوانایی از مجموعه کاراکترهای مجاز آن حذف شده‌اند. این روش کدبندی دارای سازوکاری برای ردیابی خطا است و برای کدبندی آدرس‌های سگویت و درخواست پرداخت‌های لایت‌نینگ مورد استفاده قرار می‌گیرد.

کدهای QR: از این روش کدبندی برای نمایش اطلاعات به صورت تصویری استفاده می‌شود و خروجی آن عموماً به شکل مربع‌های سیاه و سفید است. این روش برای کدبندی داده‌های طولانی که خواندن یا انتقال آن‌ها دشوار است مورد استفاده قرار می‌گیرد. اغلب تلفن‌های همراه نرم‌افزارهایی برای اسکن کدهای QR دارند. معمولاً برای نمایش آدرس‌های بیت‌کوین و درخواست پرداخت‌های لایت‌نینگ از این روش استفاده می‌شود.

رمزگذاری

Encryption

به فرآیند تبدیل داده‌های آشکار و قابل فهم به فرمتی نامفهوم رمزگذاری می‌گویند. داده‌ها به گونه‌ای رمزگذاری می‌شوند که فقط برای افراد خاصی که صلاحیت دارند قابل خواندن باشند. فرآیند رمزگذاری داده اصلی را که با نام «متن قابل خواندن» شناخته می‌شود، به یک کُد غیرقابل فهم به نام «متن رمزگذاری شده» تبدیل می‌کند. برای تبدیل «متن رمزگذاری شده» به «متن قابل خواندن» اولیه کافیت مسیر برعکس که به فرآیند «رمزگشایی» معروف است اجرا شود.

تقریباً توسط همه دستگاه‌ها و خدمات دیجیتال برای حفاظت از داده‌ها در برابر دسترسی‌های غیرمجاز و مهاجمان خراب‌کار از رمزگذاری استفاده می‌کنند. روش‌های رمزگذاری مؤثر از گذرواژه‌های کاربران محافظت می‌کند و به کاربران اجازه می‌دهد تا با خیال آسوده در اینترنت به گشت و گذار بپردازند و به یکدیگر پیام دهند.

روش‌های مختلفی برای رمزگذاری وجود دارد که هر کدام سطوح امنیت متفاوتی دارند. در اغلب موارد، برای رمزگذاری و رمزگشایی داده‌ها از یک یا چند کلید استفاده می‌شود. تعداد کلیدهایی که مورد استفاده قرار می‌گیرند و نوع آن‌ها به روش رمزگذاری انتخاب شده بستگی دارد. برخی از روش‌های رمزگذاری در برابر کامپیوترهای معمولی از امنیت پایینی برخوردارند، و برخی دیگر در برابر کامپیوترهای کوانتومی ایمن هستند.

به عنوان مثال، امروز برای همه روش است که امنیت روش رمزگذاری «سزار» که معروف است توسط جولوس سزار مورد استفاده قرار می‌گرفته، - به راحتی و با استفاده از روش تجزیه و تحلیل تکرار حروف شکسته می‌شود. آلن تورین در خلال جنگ جهانی دوم از این روش برای ساخت دستگاه انیگما و شکستن این روش رمزگذاری استفاده کرد. امروزه به نظر می‌رسد روش AES که در حال حاضر توسط سازمان امنیت ایالات متحده آمریکا استفاده می‌شود، یک روش امن برای رمزگذاری داده‌ها باشد.

اکثر روش‌های رمزگذاری امروزی از الگوی رمزگذاری نامتقارن استفاده می‌کنند. رمزگذاری نامتقارن به کاربران این اجازه را می‌دهد تا داده موردنظر را با استفاده از یک کلید عمومی رمزگذاری کنند، و رمزگشایی این داده رمزگذاری شده تنها برای کسی امکان‌پذیر است که کلید خصوصی که کلید عمومی از روی آن ساخته شده است را در اختیار داشته باشد. این قابلیت امکان برقراری ارتباط امن بر روی یک کانال ارتباطی ناامن مانند اینترنت را برای طرفین فراهم می‌کند.

فرض کنیم آوا قصد داشته باشد به بابک پیامی ارسال کند. برای این کار ابتدا بابک یک کلید خصوصی می‌سازد و از آن یک کلید عمومی استخراج می‌کند. او این کلید عمومی را برای آوا ارسال می‌کند و هیچ‌گونه نگرانی از اینکه چه کسانی به آن دسترسی پیدا می‌کنند ندارد. آوا از کلید عمومی بابک برای رمزگذاری پیام خود استفاده می‌کند و آن را برای بابک ارسال می‌کند. او نیز

هیچ گونه نگرانی از اینکه چه کسی به آن دسترسی پیدا می کند ندارد. زیرا در طول مسیر ارتباطی هیچ کس قادر به خواندن و درک پیام ارسال شده به بابک نخواهد بود. بابک پس از دریافت پیام رمزگذاری شده می تواند آن را با استفاده از کلید خصوصی خود رمزگشایی، و محتوای پیام را بخواند.

رمزگذاری سرتاسر

End-to-End (E2E) Encryption

پیام های رد و بدل شده در یک شبکه ارتباطی که ویژگی رمزگذاری سرتاسر در آن پیاده سازی شده باشد، تنها توسط فرستنده و گیرنده پیام ها قابل خواندن است. رمزگذاری سرتاسر به کاربران این امکان را می دهد که بدون نیاز به اعتماد به یک شخص یا نهاد ثالث به صورت خصوصی با دیگران ارتباط برقرار کنند.

هنگامی که یک پیام به صورت سرتاسر رمزگذاری شده باشد، فرستنده پیام آن را با استفاده از کلید عمومی گیرنده رمزگذاری می کند و هیچ شخص یا نهاد حتی گردانندگان بستر نرم افزار پیام رسانی که مورد استفاده قرار گرفته، قادر به رمزگشایی این پیام نخواهند بود. این قابلیت به کاربران این اجازه را می دهد تا برای برقراری ارتباط با یکدیگر از سرویس های متمرکز موجود استفاده کنند و هیچ گونه نگرانی بابت فاش شدن محتوای گفتگوها برای دیگران به هر دلیل ممکن، نداشته باشند.

امروزه اغلب ارتباطات دیجیتال توسط شخص یا شرکت ثالثی که در واقع نقش تسهیل کننده این ارتباط را بازی می کند، انجام می شود. هنگامی که شما برای کسی ایمیل می فرستید، این ایمیل ابتدا به سرور یک شرکت ثالث مثل گوگل فرستاده می شود، سپس این شرکت ایمیل ارسال شده را به گیرنده می فرستد. اگر ویژگی رمزگذاری سرتاسر در یک ارتباط مورد استفاده قرار نگرفته باشد، افرادی که به سرورهای سرویس به خدمت گرفته شده یا شرکت های و نهادهای ثالث به دلایل مختلف قادرند محتوای ایمیل ارسال شده را بخوانند.

به موجب مصوبه امداد اضطراری بانکداری و همچنین فرمان اجرایی ۶۱۰۲ که در سال ۱۹۳۳ تصویب شدند، حق مالکیت طلا از شهروندان آمریکایی سلب شد و آنها می‌بایست طلاهای خود را به بانک‌ها تحویل می‌دادند و در غیر این صورت مورد مجازات قرار می‌گرفتند. فرمان اجرایی ۶۱۰۲ دولت ایالات متحده آمریکا را قادر می‌ساخت تا در طول دوران رکود بزرگ بتواند از راه پایین آوردن ارزش دلار برای بازگشت رونق را به اقتصاد این کشور از روش‌های تشویقی استفاده کند. اگر شهروندان می‌توانستند از راه نگهداری از طلا از ارزش سرمایه خود محافظت کنند، این سیاست‌های تشویقی حتماً به تورم‌های بالا منجر می‌شد.

طبق این فرمان اجرایی شهروندان در قبال هر اونس طلایی که تحویل بانک می‌شد حدود ۲۰ دلار آمریکا دریافت می‌کردند. روزولت رئیس‌جمهور ایالات متحده پس از اجرایی شدن این قانون و جمع‌آوری طلای شهروندان قیمت طلا را از ۲۰ به ۳۵ دلار در ازای هر اونس افزایش داد و ارزش دلار را حدود ۵۰ درصد در طول یک روز کاهش داد.

این قانون یک رویداد منحصر به فرد نیست و موارد مشابه زیادی از مصادره عمومی طلای شهروندان در طول تاریخ رخ داده است. مصادره طلا در انگلستان، اتحاد جماهیر شوروی، و کشور کمونیستی چین مسبوق به سابقه است.

طلا مستعد مصادره شدن است، زیرا پنهان و جابجا کردن آن به دلیل فیزیکی بودن بسیار دشوار است. این ویژگی منفی صاحبان طلا را ترغیب می‌کند تا طلای خود را نزد بانک‌ها یا دیگر مؤسسات امنی نگهداری کنند. اشکال بانک‌ها و مؤسسات امنی این است که تحت فرمان دولت‌های متبوع خود هستند. مصادره طلا از میلیون‌ها شهروندی که آن را بدون واسطه در اختیار دارند از مصادره آن از بانک‌ها و مؤسساتی که گوش به فرمان دولت هستند، بسیار بسیار دشوارتر است.

F

کارمزد تراکنش بیت کوین

Bitcoin Transaction Fee

یکی از مواردی که ماینرها را به فعالیت در شبکه بیت کوین تشویق می‌کند، کسب کارمزد تراکنش‌های قرار داده شده در یک بلاک است. هرچه مقدار کارمزدی که یک تراکنش پرداخت می‌کند بیشتر باشد، ماینرها انگیزه بیشتری برای تأیید آن خواهند داشت، به عبارت دیگر این تراکنش در زمان کوتاه‌تری تأیید خواهد شد. از آنجا که فضای بلاک‌های بیت کوین محدود است، ماینرها کارمزدهای پرداخت شده در تراکنش‌ها را نسبت به فضایی که در بلاک اشغال می‌کنند در نظر می‌گیرند، نه صرفاً مقدار کارمزدی که پرداخت شده است. برای همین است که بیشتر کیف پول‌های بیت کوین مقدار کارمزد را بر اساس sats/vByte، یعنی «ساتوشی به ازای فضای مجازی اشغال شده در بلاک» نمایش می‌دهند.

کارمزد تراکنش در شبکه بیت کوین نوسانات شدیدی دارد، بعضی از تراکنش‌ها کارمزد بالایی پرداخت می‌کنند تا اطمینان داشته باشند که در زمان کوتاهی تأیید می‌شوند. اما برخی دیگر از تراکنش‌ها که عجله‌ای برای تأیید شدن ندارند، کارمزد پایینی پرداخت می‌کنند و برای تأیید شدن انتظار می‌کشند. می‌توان از راه‌های مختلفی همچون ادغام کوین‌ها و گروه‌بندی تراکنش‌ها، و به کارگیری نسخه‌های جدید تراکنش‌ها، خصوصاً سگویت در کارمزد تراکنش صرفه‌جویی کرد.

فاست

Faucet

عموماً به وب‌سایت‌هایی که بیت کوین رایگان می‌دهند فاست می‌گویند. این وب‌سایت‌ها در چند سال اول که بیت کوین ارزان بود و تقاضای چندانی نیز برای آن وجود نداشت خیلی رایج بودند. برای دریافت بیت کوین کافی بود کاربر آدرس خود را در آن‌ها وارد، و بیت کوین رایگان را دریافت کند. برخی از این فاست‌ها حتی تا چند بیت کوین به صورت رایگان به بازدیدکنندگان خود می‌دادند. گردانندگان فاست‌ها از آن به‌عنوان راهی برای گسترش آگاهی عمومی نسبت به

بیت کوین استفاده می کردند. امروزه این وبسایتها به شدت نادر هستند و اگر هم وجود داشته باشند، ارقام بسیار بسیار پایینی بیت کوین به افراد می دهند.

در حال حاضر فاستهایی برای توزیع بیت کوینهای مشقی وجود دارند. این کوینها ارزشی ندارند و فقط می توان از آنها روی شبکه تست بیت کوین استفاده کرد.

پولِ فیات

Fiat Currency

به پولهای ملی رایج در دنیا پول فیات گفته می شود که از کلمه لاتین Fiat، به معنی «تعیین شده» گرفته شده است. ارزش پول فیات توسط دولت‌هایی تعیین می شود که آن را خلق کرده اند و به عنوان وجه قانونی در معاملات می پذیرند. از آنجا که چاپ پول برای دولت‌ها هزینه ای ندارد، آنها می توانند هر وقت و به هر اندازه ای که می خواهند از آن پول، خلق کنند.

قدیمی ترین پول ملی، «پوند استرلینگ» بریتانیای کبیر است که در طول ۳۰۰ سال گذشته بیشتر از ۹۹ درصد از ارزش خود را از دست داده است. دلار آمریکا نیز در طول یک قرن گذشته حدود ۹۰ درصد ارزش خود را از دست داده است. عمر متوسط یک پول فیات حدود ۲۷ سال است.

امروزه هدف بانک‌های مرکزی که متولی پول فیات هستند، تثبیت تورم و پایین نگه داشتن آن است و همه کشورهای در دوره‌هایی از تاریخ در این کار موفق بوده اند. با این حال بیشتر پول‌ها در بلندمدت از تورم مصون نمانده اند و این مسأله برای کسانی که پول‌شان را پس انداز می کنند مشکل ساز است.

فورک (انشعاب)

Fork

یک فورک زمانی اتفاق می افتد که بخشی از یک پروتکل یا قسمتی از کُد یک نرم افزار بعد از اجرای عملیات ارتقاء یا به روزرسانی، تغییر کند. فورک‌ها در حوزه نرم افزار و پروژه‌های اپن سورس رخ می دهند زیرا کاربران هر زمان بخواهند می توانند نسبت به داندلود و اجرای نسخه‌های مختلف این

نرم افزارها اقدام کنند و همه کاربران یک نرم افزار لزوماً نسخه آخر آن را دریافت نمی کنند. اگر دو کاربر نسخه اول یک نرم افزار را دانلود و آن را اجرا کنند، و فقط یکی از آن ها پس از منتشر شدن نسخه دوم این نرم افزار آن را به روزرسانی کند، کاربری که نرم افزار خود را به نسخه بعدی ارتقاء داده، یک فورک از نسخه اول را اجرا می کند.

این مسأله می تواند برای سیستم هایی مانند بیت کوین که در آن برای تعیین دارایی افراد نیاز به اجماع است، مشکل ساز باشد. اگر نودهای شبکه نرم افزارهای متفاوتی اجرا، و در نتیجه قوانین پروتکل متفاوتی بر روی شبکه اعمال کنند، ممکن است روی معتبر بودن یا نبودن برخی از بلاک ها و تراکنش ها در شبکه بیت کوین با یکدیگر به توافق نرسند. در این صورت شبکه دچار از هم گسیختگی و توافق روی دفتر کل غیرمتمرکز بیت کوین - که اصلی ترین حقیقت موجود در شبکه بیت کوین است - خدشه دار خواهد شد. دلیل انتخاب روش توسعه محافظه کارانه و محتاط بودن توسعه دهندگان بیت کوین نیز همین است.

فورک ها اساساً به دو شکل وجود دارند: سافت فورک و هارد فورک. ارتقاء قوانین شبکه از راه سافت فورک - به شرط حمایت اکثریت قریب به اتفاق ماینرها، - موجب از بین رفتن سازگاری بین نسخه های قدیمی و جدید نمی شود. بنابراین لازم نیست همه نودهای شبکه در این روش نرم افزار خود را به روزرسانی کنند زیرا قوانین نسخه جدید ویژگی پس سازگاری دارند. در مقابل هارد فورک ها این ویژگی را ندارند، بنابراین برای به منظور ارتقاء قوانین شبکه همه نودها مجبور به به روزرسانی نرم افزار خود هستند. فعالان بیت کوین تا حد ممکن از اجرای هارد فورک اجتناب می کنند و به شدت به سافت فورک ها علاقه مندند.

هنگامی که یک پروژه برای به روزرسانی قوانین پروتکل از روش هارد فورک استفاده کند و بخشی از کاربران همچنان نسخه قدیمی را اجرا کنند، شبکه دچار از هم گسیختگی و به دو شاخه تقسیم می شود. این اتفاق چندین بار در شبکه بیت کوین رخ داده است، زیرا برخی از پروژه ها تلاش کرده اند تا از قوانین پروتکل بیت کوین خارج شوند و آن را برای خود تغییر دهند. به این پروژه ها که از قوانین پروتکل بیت کوین سرپیچی کرده اند نیز فورک گفته می شود، اما آن ها دیگر بخشی از پروژه بیت کوین و شبکه آن نیستند. این پروژه ها ممکن است موجب به وجود آمدن سردرگمی

اجتماعی شوند اما در سطح پروتکل تهدیدی برای بیت کوین به شمار نمی آیند.

فانجیل بودن (تعویض پذیری)

Fungibility

یک ویژگی برای کالاهایی است که می توان آن ها را با یکدیگر تعویض کرد و وقتی کنار هم قرار می گیرند نمی توان آن ها را از یکدیگر تمیز دارد. بهترین نمونه از یک کالای فانجیل، سکه هایی است که در گذشته به عنوان پول خرد مورد استفاده قرار می گرفت اما در حال حاضر با توجه به کاهش ارزش پول تقریباً منسوخ شده اند. به عنوان مثال هر کدام از سکه های ۵۰۰ تومانی که در گذشته رایج بودند، ۵۰۰ تومان ارزش داشتند و برای کسی که ۵۰۰ تومان از شما طلب داشت فرقی نمی کرد کدام یک از سکه های ۵۰۰ تومانی خود را به او بدهید.

فانجییلیتی یکی از ویژگی های مطلوب بیت کوین است زیرا کارآمدی آن را به عنوان یک ابزار پرداخت برای عموم افراد بیشتر می کند. به عنوان مثال اگر کوین هایی که در گذشته در مالکیت مجرمان بوده اند را بتوان از بقیه کوین ها تمیز داد، ممکن است صرافی ها و فروشندگان تمایلی برای پذیرش آن ها نداشته باشند. در این صورت پذیرندگان بیت کوین باید برای اطمینان از لکه دار نبودن کوین ها، هر کدام از آن ها را به صورت جداگانه مورد بررسی قرار دهند. این محدودیت ها با توجه به دشواری هایی که برای کاربران، پذیرندگان، صرافی ها به وجود می آورد، عموم مردم را از پذیرش و استفاده از بیت کوین دلسرد و ناامید خواهد کرد.

راه حل های حفظ حریم خصوصی مانند کوین جوین با مخفی نمودن مالکان قبلی یک کوین از راه های مطمئن و امن، برای فانجیل بودن بیت کوین، و بی معنی شدن مفهوم کوین های لکه دار، تلاش می کنند.

نظریه بازی مطالعه ریاضی تضادها و استراتژی‌هایی است که برای اتخاذ مؤثرترین تصمیم بر اساس قوانین از پیش تعیین شده، مورد تحلیل قرار می‌گیرد. این نظریه به عنوان یک ساختار ارزشمند برای مفهوم آفرینی فرآیند تصمیم‌گیری عمل می‌کند.

معمای زندانی

معمای زندانی نشان می‌دهد که چگونه ممکن است دو نفر با یکدیگر همکاری نکنند، هرچند همکاری به نفع آن‌ها باشد. بر اساس این قیاس نظریه بازی، دو زندانی دستگیر شده‌اند و در انتظار محاکمه هستند. هر کدام از آن‌ها دو راه دارند: به دیگری خیانت کنند یا سکوت کنند. اگر هر دو زندانی به یکدیگر خیانت کنند، هر کدام به دو سال حبس محکوم خواهند شد. اگر هر دو سکوت کنند، هر دو به یک سال حبس محکوم خواهند شد. اگر یکی از زندانیان خیانت کند و دیگری سکوت کند، آن زندانی که سکوت کند، مجازات کامل که سه سال حبس است را خواهد گرفت. بر این اساس، یک زندانی منطقی برای حفاظت از خود به دیگری خیانت خواهد کرد، حتی اگر راه حل بهینه برای آن‌ها این باشد که با یکدیگر همکاری، و سکوت کنند.

مسأله ژنرال‌های بیزانس

مسأله ژنرال‌های بیزانس یکی از قیاس‌های معروف نظریه بازی است. این مسأله با حمله تعدادی از ژنرال‌ها به بیزانس آغاز می‌شود. آن‌ها شهر را محاصره کرده‌اند و باید به اتفاق برای تعیین زمان حمله به شهر تصمیم بگیرند. ژنرال‌ها راهی برای برقراری یک ارتباط امن با یکدیگر ندارند و هر پیامی که ارسال یا دریافت می‌کنند ممکن است توسط مدافعان شهر بیزانس شنود شود، یا برای گمراه کردن آن‌ها از طرف مدافعان شهر ارسال شده باشد. اگر همه ژنرال‌ها به طور همزمان به شهر حمله

کنند پیروز میدان خواهند بود، اما اگر حمله در زمان‌های متفاوت انجام پذیرد جنگ را خواهند باخت.

سیستم‌های غیرمتمرکز با مسئلهٔ ژنرال‌های بیزانس مواجه هستند زیرا هیچ نهاد متمرکزی وجود ندارد تا اطلاعات را برای اعضای شبکه تأیید کند. سیستم‌های متمرکز با این مشکل مواجه نیستند زیرا اعضای شبکه خطر اعتماد به یک واسطه را می‌پذیرند و این قیاس نظریهٔ بازی برای آن‌ها موضوعیت ندارد. همین‌طور اگر ژنرال‌های بیزانس می‌توانستند برای تعیین زمان حمله به یک واسطه اعتماد کنند، این قیاس نظریهٔ بازی اصلاً به‌وجود نمی‌آمد.

ساتوشی ناکاموتو، خالق ناشناس بیت کوین برجسته‌ترین نقص پول فیات را اینگونه توضیح می‌دهد: «مشکل ریشه‌ای پول‌های رایج این است که باید به آن‌ها اعتماد کنیم تا کارایی داشته باشند.»

امروزه مسئلهٔ ژنرال‌های بیزانس به طور فزاینده‌ای محبوب شده است زیرا الگوریتم اثبات کار بیت کوین اولین راه درست نظری برای حل این مشکل است. پول‌های غیرمتمرکز با مسئلهٔ ژنرال‌های بیزانس مواجه هستند و باید بر آن غلبه کنند، زیرا گروه غیرمتمرکز کاربران می‌بایست روی درستی تاریخچهٔ تراکنش‌ها و درستی سیاست پولی تعیین شده به اجماع برسند.

Generator Point

نقطهٔ مولد

نقطهٔ مولد که با نماد G شناخته می‌شود، نقطه‌ای است که روی منحنی بیضوی secp256k1 بیت کوین تعریف شده و دارای مختصات x و y است. یک کاربر برای تولید کلید عمومی، کلید خصوصی خود را در G ضرب می‌کند.

$$sk * G = P$$

کلید خصوصی یک عدد بزرگ است، اما کلید عمومی نقطه‌ای با مختصات x و y است. عدد G نیز خود یک کلید عمومی معتبر است.

رابط کاربری گرافیکی، یک برنامه نرم‌افزاری است که به کاربران اجازه می‌دهد به صورت بصری با نرم‌افزاری که در لایه پایین تر قرار دارد تعامل داشته باشند. در غیاب رابط کاربری گرافیکی کاربران مجبور به استفاده از خط فرمان (ترمینال) هستند. رابط‌های کاربری گرافیکی با فراهم کردن امکان تعامل بصری تلاش می‌کنند تا پیچیدگی‌های نرم‌افزارها را از دید کاربران پنهان کنند. اغلب برنامه‌هایی که رابط کاربری گرافیکی دارند را می‌توان بدون رابط کاربری گرافیکی از طریق خط فرمان (ترمینال) نیز به خدمت گرفت.

اکثر نرم‌افزارهای بیت‌کوین از جمله بیت‌کوین‌گر که رابط کاربری آن با نام بیت‌کوین کیوت شناخته می‌شود، دارای رابط کاربری گرافیکی هستند. همچنین اغلب کیف پول‌های بیت‌کوین دارای رابط کاربری گرافیکی هستند.

Gresham's Law

قانون گرشام

قانون گرشام بیان می‌کند که «پول بد، پول خوب را از دور خارج می‌کند». به عبارت دیگر، در اقتصادی که دو پول متفاوت در آن در گردش باشد، افراد پول بد که ارزش آن دائماً کاهش می‌یابد را خرج، و پول خوب که ارزش خود را حفظ می‌کند را نگه می‌دارند. بنابراین پول بد بیشتر در معاملات روزمره، و پول خوب بیشتر برای پس‌انداز و سرمایه‌گذاری بلند مدت به کار گرفته می‌شود.

به عنوان مثال، فردی را در نظر بگیرید که هم بیت‌کوین و هم ریال دارد. اگر او بخواهد پولش را برای خرید کالا خرج کند، ترجیح می‌دهد ریال را خرج کند زیرا ارزش ریال دائماً در حال کاهش است. اگر بیت‌کوین خود را خرج کند، با افزایش احتمالی ارزش بیت‌کوین متضرر خواهد شد. یکی از دلایلی که موجب شده بیت‌کوین بیش از آنکه ابزاری برای پرداخت باشد، به عنوان ابزاری برای ذخیره ارزش مورد استفاده قرار می‌گیرد نیز همین است.

قانون گرشام در مواقعی که ارزش پول توسط قوانین دولت یا بانک مرکزی تعیین می‌شود، به خوبی

قابل مشاهده است. به عنوان مثال دولت ایالات متحده آمریکا در سال ۱۹۶۵ مقدار نقره موجود در سکه‌های نیم دلاری را از ۹۰ به ۶۰ درصد کاهش داد. هر دوی این سکه‌ها از نظر قانونی ارزش یکسانی داشتند، بنابراین دارندگان سکه‌هایی که خلوص بالاتری داشتند آن‌ها را ذوب و به خارج از کشور صادر، یا آن‌ها را از دور خارج و به عنوان ابزاری برای حفظ ارزش استفاده می‌کردند.

قانون گرشام توضیح می‌دهد که چگونه دخالت دولت در عرضه و ارزش‌گذاری پول می‌تواند به اقتصاد آسیب بزند.

H

هَویَنگ

Halving

رویدادی است که تقریباً هر چهار سال یک بار اتفاق می‌افتد و نرخ تولید بیت کوین‌های جدید در هر بلاک را به نصف کاهش می‌دهد. جزئیات زمان‌بندی خلق بیت کوین‌های جدید، توسط الگوریتمی در کُد آن تعریف شده است. این الگوریتم به ماینرها اجازه می‌دهد تا مقدار معینی بیت کوین جدید در هر بلاک به‌عنوان یارانه ساخت بلاک و به‌منظور جبران هزینه‌ها خلق و به حساب خود واریز کنند.

در ابتدای کار شبکه بیت کوین، یارانه ساخت هر بلاک ۵۰ بیت کوین بوده است. با این حال، رویدادی که به هویَنگ معروف است هر ۲۱۰,۰۰۰ بلاک تقریباً هر چهار سال رخ می‌دهد و مقدار این یارانه به نصف کاهش می‌یابد. این روند تا زمانی ادامه پیدا می‌کند که یارانه ساخت بلاک به صفر برسد، زمانی که بیش از ۷ میلیون بلاک در ۳۴ هویَنگ ساخته شده است.

سقف عرضه

Hard Cap

مجموع عرضه بیت کوین هرگز از ۲۱ میلیون بیت کوین یا ۲۰۱ کوادریلیون ساتوشی تجاوز نخواهد کرد. سقف عرضه یک ویژگی است که کمیابی مطلق بیت کوین را تضمین می‌کند و موجب می‌شود بیت کوین به سرنوشت بسیاری از پول‌های فیات که همانا اَبَر تورم است، دچار نشود.

کالای سخت

Hard Commodity

معمولاً به منابع طبیعی مانند فلزات گران‌بها و موارد خاصی از ذخایر انرژی که از روش استخراج تولید می‌شوند، کالاهای سخت گفته می‌شود. طلا، نقره، و نفت برخی از رایج‌ترین کالاهای سخت هستند.

به طور کلی فورک یعنی ایجاد یک تغییر در سورس کُد یک پروژه نرم‌افزاری. بیت کوین یک پروژه متن باز (اپن سورس) است، به این معنی که هرکسی بدون نیاز به کسب اجازه به کُد آن دسترسی دارد، می‌تواند آن را دانلود کند و آن را تغییر دهد.

به طور خاص هارد فورک یعنی اعمال تغییراتی در قوانین، به نحوی که امکان فراهم کردن ویژگی پسا سازگاری در شبکه وجود نداشته باشد. اگر اموری که طبق قوانین فعلی شبکه نامعتبر هستند پس از اعمال تغییر در کُد نرم‌افزار (فورک) و بر طبق قوانین جدید معتبر شوند، این فورک در اصل یک هارد فورک است. به منظور حفظ اجماع پس از اعمال یک هارد فورک، همه نودهای (گره) شبکه می‌بایست نرم‌افزار نودهای خود را به‌روزرسانی کنند. در غیر این صورت تراکنش‌ها و بلاک‌هایی که با قوانین جدید ساخته شده‌اند از نظر نودهایی که نرم‌افزار قدیمی را اجرا می‌کنند نامعتبرند، در حالی که نودهای به‌روزرسانی شده آن‌ها را به عنوان بلاک‌ها و تراکنش‌های معتبر می‌پذیرند. به همین دلیل است که در روند ارتقاء پروتکل بیت کوین تا جایی که ممکن باشد از اعمال هارد فورک اجتناب می‌شود.

کیف پول سخت‌افزاری

Hardware Wallet

کیف پول سخت‌افزاری یک دستگاه دیجیتال است که تنها هدف آن تولید و ذخیره کلیدهای عمومی و خصوصی و امضای تراکنش‌ها است. کیف پول‌های سخت‌افزاری به کاربران این امکان را می‌دهند تا بیت کوین‌های خود را به روشی امن دریافت و ارسال کنند. کیف پول‌های سخت‌افزاری نوعی کلد استوریج هستند، به این معنی که کاربران را قادر می‌سازند تا از کلیدهای خصوصی خود در شرایطی ایمن و به دور از اینترنت نگهداری کنند.

اغلب کیف پول‌های سخت‌افزاری استانداردهای بیپ-۳۲ و بیپ-۳۹ را پیاده‌سازی کرده‌اند، به این معنی که از قابلیت‌های کیف پول‌های سلسله‌مراتبی قطعی و کلمات بازیابی پشتیبانی می‌کنند. کیف پول‌های سخت‌افزاری مختلف از نظر امنیت، حریم خصوصی، و قابلیت اطمینان با یکدیگر متفاوت

توابع هَش

Hash Function

تنوع توابع هَش بسیار بالاست، اما توابع هَش به کار گرفته شده در حوزه رمزنگاری در ویژگی‌های کلیدی زیر مشترک هستند.

- همه توابع هَش یک پارامتر ورودی (معروف به preimage) می‌گیرند و یک خروجی به نام هَش (معروف به digest) با طول ثابت تولید می‌کنند. این طول بر اساس تابع هَش انتخاب شده متفاوت است.
- خروجی یک تابع هَش قطعی است. این بدان معنا است که برای یک ورودی مشخص، خروجی همواره یکسان خواهد بود.
- توابع هَش یک‌طرفه هستند. این بدان معنا است که با فرض در اختیار داشتن ورودی، می‌توان خروجی را به آسانی تولید کرد. هیچ راهی برای به‌دست آوردن ورودی از روی خروجی یک تابع هَش وجود ندارد.
- خروجی یک تابع هَش تصادفی و غیر قابل پیش‌بینی است و میان مجموعه‌ای از ورودی‌ها و خروجی‌ها هیچ رابطه‌ای وجود ندارد. برای نمونه اگر فقط یک کاراکتر از یک ورودی ۱۰۰ کاراکتری تغییر کند، خروجی ورودی دوم هیچ‌گونه شباهتی به خروجی اول نخواهد داشت.

این ویژگی‌های توابع هَش در بیت‌کوین کاربرد دارند. برای نمونه ویژگی تصادفی و غیرقابل پیش‌بینی بودن آن‌ها، استخراج بیت‌کوین را به یک رقابت منصفانه تبدیل می‌کند. به‌دست آوردن آدرس‌های بیت‌کوین از راه هَش کردن کلید عمومی یا اسکرپت، امنیت، حریم خصوصی، و راحتی را برای کاربران به ارمغان می‌آورد. هَش کردن تراکنش‌ها و بلاک‌ها روشی ساده برای ایجاد شناسه‌های غیرتکراری برای آن‌ها می‌شود. در نهایت این توابع برای محاسبه درخت مرکب به کار گرفته می‌شوند. درخت مرکب خلاصه‌ای قابل اعتماد و غیرقابل تغییر از تمام تراکنش‌هایی که در یک بلاک وجود دارند، می‌سازد و موجب بهینه‌تر شدن روند تأیید اعتبار تراکنش‌ها و بلاک‌ها می‌شود.

انواع توابع هش کاربردهای مختلفی در بیت کوین دارند. تابع هش SHA-256 برای تولید عدد اثبات کار و همچنین برای تولید شناسه تراکنش، دو بار پشت سر هم به کار گرفته می شود.

از تابع هش HASH160 برای تولید هش کلیدهای عمومی یا آدرس های قدیمی بیت کوین استفاده می شود. این تابع ترکیبی از دو تابع هش SHA-256 و RIPEMD160 است.

مقدار هش

Hash Rate

عددی است که نشان می دهد ماینرهای شبکه بیت کوین در مجموع قادر به محاسبه چند هش بر واحد ثانیه هستند. هر یک بار هش، تلاشی برای تولید عدد اثبات کار یک بلاک معتبر است و ماینرهای شبکه بیت کوین در سراسر جهان در هر ثانیه میلیاردها بار برای به دست آوردن آن تلاش می کنند. مقدار هش نشان می دهد که چه مقدار پول، انرژی، و توان محاسباتی به پردازش تراکنش ها و ایمن سازی شبکه بیت کوین اختصاص داده شده است.

همچنین می توان از روی مقدار هش، هزینه اجرای یک حمله ۵۱ درصد به شبکه بیت کوین را با تقریب خوبی تخمین زد. زیرا اجرای یک حمله ۵۱ درصد مستلزم آن است که ۵۱ درصد مقدار هش شبکه در اختیار یک ماینر خراب کار باشد و هرچه مقدار هش بیشتر باشد، اجرای چنین حمله ای نیز گران تر خواهد بود و احتمال اجرای این حمله کاهش خواهد یافت.

مقدار هش بیت کوین در دهه گذشته با سرعت زیادی رشد کرده است، زیرا افزایش قیمت بیت کوین ماینرهای بیشتری را برای پیوستن به شبکه ترغیب می کند. مقدار هش تحت تأثیر عوامل مختلفی از جمله قیمت بیت کوین، قیمت انرژی، آب و هوا، و قوانین محلی است.

هگزادسیمال

Hexadecimal

هگزادسیمال یک روش گدبندی است که از یک الفبای ۱۶ کارا کتری، شامل ارقام ۰ تا ۹ و حروف A-F استفاده می کند. کوچک یا بزرگ بودن حروف در این طرح اهمیتی ندارد و اغلب داده هایی که

با این روش کُدبندی می‌شوند پیشوند «0x» دارند. داده‌هایی چون کلیدهای عمومی، تراکنش‌ها، هَش‌ها، و اسکرپیت بیت‌کوین از این روش کُدبندی و نمایش داده می‌شوند.

Hierarchical Deterministic (HD) Wallet

کیف پول اچ‌دی (سلسله‌مراتبی قطعی)

کیف پول سلسله‌مراتبی قطعی اصطلاحی است که برای توصیف کیف پول‌هایی به کار می‌رود که از یک بذر (سید) برای تولید کلیدهای عمومی و خصوصی استفاده می‌کنند. این نوع کیف پول‌ها در پیشنهاد بهبود بیت‌کوین شماره ۳۲ معرفی، و سپس به‌عنوان یک استاندارد در بیت‌کوین پیاده‌سازی شدند. اکثر کیف پول‌ها قبل از به کارگیری این استاندارد، برای تولید یک آدرس جدید بیت‌کوین جفت کلید جدیدی تولید می‌کردند که ارتباطی با کلیدهای تولید شده قبلی نداشت. کاربران برای پشتیبان‌گیری از این کیف پول‌ها که کلیدهایشان را از این روش که به روش «مجموعه‌ای از کلیدهای نامرتب با یکدیگر» معروف است می‌ساختند، مجبور بودند از تک تک کلیدها پشتیبان‌گیری کنند و این موضوع دردسرهای قابل توجهی هم برای سازندگان کیف پول‌ها، و هم کاربران به وجود می‌آورد. اما کیف پول‌های سلسله‌مراتبی قطعی را می‌توان به آسانی و با ذخیره یک داده ۶۴ بیتی -متشکل از یک کلید خصوصی ۳۲ بیتی، به علاوه ۳۲ بایت داده تصادفی، معروف به بذر (سید)، پشتیبان‌گیری کرد. برای جلوگیری از اشتباهاتی که ممکن است در روند ذخیره و بازیابی داده باینری بذر (سید) رخ دهد، پیشنهاد بهبود بیت‌کوین شماره ۳۹ معرفی شد و در حال حاضر توسط اکثر کیف پول‌های بیت‌کوین مورد استفاده قرار می‌گیرد. در این روش بذر (سید) در قالب ۱۲ تا ۲۴ کلمه یادآوری به کاربر نمایش داده می‌شود و در اختیار داشتن این کلمات برای بازیابی کیف پول کفایت می‌کند.

اصطلاح سلسله‌مراتبی، ساختار درختی مانند کلیدها را توصیف می‌کند: کلید اصلی از بذر (سید) کیف پول مشتق می‌شود و برای تولید کلیدهای فرزند به کار گرفته می‌شود که هر کدام مجدداً قادرند به‌طور مستقل کلیدهای فرزند خود را تولید کنند.

هریک از این کلیدهای مشتق شده (فرزندان) را می‌توان با مسیر استخراج آن توصیف کرد، که حاوی اطلاعاتی در مورد عمق و جایگاه این کلید در ساختار درختی کلیدها است. یک کیف پول

اچدی اطلاعاتی که در مسیر استخراج قرار دارد را به کار می گیرد و کلید مورد نظر را استخراج می کند. کلید اصلی که از بذر (سید) مشتق می شود را با حرف m نمایش می دهند. برای مثال، فرزند اول کلید اصلی دارای مسیر استخراج "m/0" است، و مسیر استخراج فرزند پنجم اولین فرزند "m/0/4" است.

قطعی بودن این درخت بدان معنا است که یک بذر (سید) یا یک کلید اصلی (m) همیشه دقیقاً درخت یکسانی از کلیدها را خواهد ساخت. همچنین یک کلید اصلی و یک مسیر استخراج مشخص، همیشه کلیدهای یکسانی را تولید خواهد کرد. این قابلیت به کاربران کیف پولهای اچدی این امکان را می دهد که نسخه پشتیبان را تنها با ذخیره بذر (سید) تهیه کنند و نیازی به پشتیبان گیری از صدها کلید نامرتبط با یکدیگر نباشد. این قابلیت همچنین کاربران را قادر می سازد تا آدرسهای جدید را بدون نیاز به کلید خصوصی و از راه به کارگیری کلید عمومی والد که با نام کلید عمومی بسط یافته یا xpub نیز شناخته می شود، تولید کنند. این بدان معنی است که کاربر می تواند کلیدهای خصوصی خود را به روش کلداستوریج نگهداری کند، در حالی که با وارد کردن کلیدهای عمومی خود در یک کیف پول آنلاین و تولید آدرسهای جدید قادر است به راحتی بیت کوین دریافت کند. کیف پولی که کلید عمومی اصلی یا xpub در آن وارد شده است، به کیف پول ناظر معروف است، زیرا تنها امکان دریافت بیت کوین و نمایش موجودی کیف پول را دارد و با توجه به در اختیار نداشتن کلیدهای خصوصی قادر به امضاء کردن تراکنشها نیست.

هودل

HODL

هودل در جامعه بیت کوین شبیه به یک ضرب المثل است که از غلط املائی کلمه hold گرفته شده و به بیت کوینرها توصیه می کند در مواجهه با نوسانات شدید قیمتی که بیت کوین اغلب تجربه می کند، از فروش خودداری کنند. منشاء عبارت هودل مطلبی است که یک بیت کوینر مست در یکی از انجمنهای سایت bitcointalk و در خلال یکی از سقوطهای قیمتی بیت کوین نوشته است.

کیف پول داغ (آنلاین)

Hot Wallet

کلمه داغ اشاره به آنلاین بودن دارد، بنابراین کیف پول داغ کیف پولی است که به شبکه بیت کوین متصل باشد. معمولاً برای دریافت و پرداخت‌های روزمره از این کیف پول‌ها استفاده می‌شود، اما باید توجه داشت که برای نگهداری بلندمدت از مقادیر زیادی از بیت کوین به اندازه روش نگهداری کلداستوریج امن نیستند. هر وسیله‌ای که با اینترنت تعامل دارد ممکن است هدف نرم‌افزارهای مخرب اینترنتی قرار گیرد و دارایی افراد را به خطر اندازد.

آبر تورم

Hyperinflation

به تورم بسیار بالایی که در نتیجه افزایش شدید قیمت‌ها در یک دوره کوتاه پدید می‌آید، آبر تورم گفته می‌شود. آستانه آبر تورم در اقتصادهای مختلف متفاوت است اما اغلب در دوران بی‌ثباتی اقتصاد، زمانی که دولت‌ها با سرعت بالایی پایه پولی را افزایش می‌دهند اتفاق می‌افتد. اقتصادها نمی‌توانند در مقابل دوره‌های پایدار و طولانی آبر تورم دوام بیاورند، یا سطح تورم به سطوح قابل قبول بازگردانده می‌شود، یا سیستم مالی سقوط می‌کند، و دولت ناگزیر به تغییر واحد پولی یا حتی در مواردی معرفی یک پول جدید خواهد بود.

بیت کوین سطح بالایی از خداشه ناپذیری را در دو سطح حفظ می کند. سطح اول، اجماع و جنبه های اصلی پروتکل به خصوص سیاست پولی سخت گیرانه بیت کوین است که تغییر نمی کند. خداشه ناپذیری در این سطح توسط ده ها هزار نود بیت کوین که به طور مستقل یک کد مشترک را اجرا می کنند و بر روی مجموعه ای از قوانین مشترک با یکدیگر توافق دارند، اعمال می شود. هیچ فرد یا نهادی، نه ماینرها، و نه دولت ها بدون متقاعد کردن این ده ها هزار نود برای موافقت با تغییرات پیشنهادی، قادر به تغییر قوانین اجماع بیت کوین نخواهد بود. حفظ قابلیت خداشه ناپذیری در این سطح موجب اعتماد سرمایه گذاران کلان و خرد نسبت به کمیابی و دوام بیت کوین می شود.

سطح دوم، زنجیره بلاک است که بازنویسی (یا تغییر) تاریخچه نقل و انتقال بیت کوین را عملاً غیرممکن می کند. حفظ خداشه ناپذیری در این سطح موجب می شود تا فروشندگان و تجار از بیت کوین به عنوان یک ابزار مبادله استفاده کنند و حتی بیشتر از پول های فیات به آن اعتماد داشته باشند. زنجیره بلاک بیت کوین به گونه ای طراحی و پیاده سازی شده است که فقط می توان بلاک های جدید به آن اضافه کرد، یعنی پس از اضافه شدن یک بلاک به زنجیره، حذف یا تغییر آن عملاً غیرممکن است. این ویژگی توسط عملگر هَش SHA-256 اعمال، و موجب خداشه ناپذیری تاریخچه بیت کوین می شود. هنگامی که یک ماینر یک بلاک را به امید یافتن یک اثبات کار معتبر هَش می کند، هَش بلاک قبل در آن گنجانده شده است. به لطف ویژگی های توابع هَش، اگر هَش یک بلاک در نتیجه اعمال تغییرات در تراکنش های آن تغییر کند، عدد اثبات کار بلاک مورد نظر و در نتیجه کل بلاک و بلاک های بعد از آن نامعتبر خواهند شد.

به عنوان مثال، اگر زنجیره بلاک دارای ۵۰۰ بلاک باشد، هَش بلاک شماره ۴۰۰ شامل هَش بلاک شماره ۳۹۹ است. اگر بلاک شماره ۳۹۹ کوچک ترین تغییری کند در نتیجه هَش آن نیز تغییر خواهد کرد و باعث تغییر هَش بلاک بعدی یعنی بلاک شماره ۴۰۰ خواهد شد و این روند تا نامعتبر

شدن آخرین بلاک یعنی بلاک شماره ۵۰۰ در زنجیره ادامه پیدا می کند. تغییر یک بلاک در زنجیره بلاک بیت کوین، منجر به نامعتبر شدن همه بلاک های بعد از آن خواهد شد، این یعنی ایجاد تغییر در زنجیره بلاک بیت کوین بدون بازنویسی بخشی از تاریخچه بلاک های زنجیره ممکن نیست.

اگر یک مهاجم اکثریت کل توان محاسباتی شبکه بیت کوین را در اختیار داشته باشد می تواند بلاک های زنجیره بیت کوین را تغییر، و تاریخچه زنجیره را از طریق حمله ۵۱ درصدی بازنویسی کند. برای اینکه هزینه اجرای چنین حمله ای فراتر از توان هر نهاد یا دولتی باشد، شبکه بیت کوین به میزان هش بالا و غیرمتمرکز نیاز دارد.

تورم

Inflation

تورم، افزایش تدریجی قیمت اجناس در اقتصاد یک کشور است و باعث پایین آمدن قدرت خرید مردم می شود. تورم در اقتصادهای مدرن به عنوان یک امر پیش بینی شده در نظر گرفته می شود و دلیل به وجود آمدن آن عمدتاً رشد مداوم پایه پولی توسط دولت های محلی یا بانک های مرکزی است. هنگامی که تورم به سطوح بالایی برسد، به آرتورم تبدیل می شود.

تورم به طور کلی بر اساس متوسط قیمت کالاهای مشخصی که در سبد خانوار قرار دارند محاسبه می شود، و شاخص قیمت مصرف کننده نام دارد. پول های فیات ارزش خود را به دلیل تورم در طول زمان از دست می دهند و ابزار مناسبی برای حفظ ارزش دارایی صاحبان خود نیستند.

دانلود زنجیره بلاک برای بار اول

Initial Block Download (IBD)

به فرآیند دانلود زنجیره بلاک بیت کوین برای بار اول گفته می شود. هنگامی که یک نود (گره) جدید که به تازگی راه اندازی شده برای اولین بار به شبکه بیت کوین می پیوندد، ابتدا به نودهای دیگر وصل می شود و سپس درخواست دانلود زنجیره بلاک را به آنها ارسال می کند. این نود جدید فرآیند دانلود و پردازش زنجیره بلاک را از اولین بلاک شروع، و تا آخرین بلاک ادامه می دهد و به اصطلاح با شبکه همگام می شود.

در این فرآیند، با وجود اینکه بلاک‌ها از نودهای متفاوتی در شبکه دریافت می‌شوند نیازی به اعتماد به آن‌ها نیست. زیرا هر نود می‌تواند داده‌ها را از نودهای مختلف دریافت و به‌طور مستقل صحت آن‌ها را از راه مقایسه بسنجد، همچنین به دلیل ماهیت زنجیره بلاک‌ها که بر اساس اثبات کار است، هر نود می‌تواند به‌صورت مستقل و بدون نیاز به اعتماد به نودهای دیگر، بلاک‌های دریافت شده را اعتبارسنجی کند. این فرآیند می‌تواند بسته به سرعت ارتباط با شبکه اینترنت و مشخصات سخت‌افزاری دستگاهی که نرم‌افزار بیت‌کوین را اجرا می‌کند، از یک تا چند ده روز زمان ببرد.

هنگامی که این فرآیند آغاز می‌شود، نود مورد نظر ابتدا تمام سربرگ‌های بلاک‌های زنجیره را از نودهایی که به آن‌ها وصل شده است، دریافت و سپس به داندلود بلاک‌ها می‌پردازد. این کار موجب بهینه شدن فرآیند داندلود بلاک‌ها می‌شود و همچنین برخی از قابلیت‌های کاربردی را از همان ابتدا برای کاربر آن فراهم می‌کند. یک نود بیت‌کوین در کنار انجام فرآیند داندلود و ساخت زنجیره بلاک، نسبت به ایجاد مجموعه خروجی‌های خرج نشده (UTXO) اقدام می‌کند. این مجموعه لیست جامعی از تمام کوین‌های معتبر در شبکه بیت‌کوین است که هنوز خرج نشده‌اند و هریک از نودهای شبکه به محض دریافت یک بلاک جدید، این مجموعه را به‌روزرسانی می‌کنند.

توالی ورودی (انسیکوئنس) Input Sequence (nSequence)

توالی ورودی یکی از فیلدهای تعریف شده در ورودی تراکنش‌ها است که در ابتدا برای فعال کردن کانال‌های پرداخت، -مشابه با شبکه لایتینگ- در نظر گرفته شده بود. این طرح در اولین نسخه بیت‌کوین پیاده‌سازی شد، اما بعد از مدت کوتاهی مشخص شد که کانال‌های پرداخت روی زنجیره اصلی از امنیت لازم برخوردار نیستند. بنابراین، این فیلد سال‌ها بدون استفاده باقی ماند.

با پیاده‌سازی پیشنهاد بهبود بیت‌کوین به شماره ۱۲۵ (بیپ-۱۲۵) این فیلد مجدداً مورد استفاده قرار گرفت و در حال حاضر به‌منظور سیگنال‌دهی برای جایگزینی تراکنش با کارمزد بالاتر استفاده می‌شود. این قابلیت به کاربر این اجازه را می‌دهد که یک تراکنش تأیید نشده را با تراکنش مشابهی که کارمزد بالاتری می‌پردازد، جایگزین کند. اگر یک کاربر تراکنشی را با کارمزد پایین به شبکه ارسال کند و این تراکنش در زمان دلخواه او تأیید نشود، او می‌تواند با استفاده از این قابلیت کارمزد

تراکنش را افزایش دهد و ماینرها را به تأیید تراکنش مورد نظر تشویق کند.

K

احراز هویت مشتری

Know Your Customer (KYC)

قوانین احراز هویت مشتریان برای جلوگیری از سوءاستفاده‌های احتمالی مشتریان از مؤسسات مالی و انتقال غیرقانونی پول تدوین شده‌اند. این قوانین تقریباً برای همه مؤسسات مالی -مانند صرافی‌ها و کارگزاری‌ها- که سرمایه مشتریان خود را در اختیار دارند، لازم‌الاجرا است. قوانین احراز هویت مشتریان جزئی از قوانین مبارزه با پول‌شویی هستند و نحوه اجرای آنها در حوزه‌های قضایی مختلف متفاوت است.

L

معماری لایه‌ای

Layered Architecture

ظرفیت پردازش شبکه بیت کوین به‌طور متوسط بین ۴ تا ۷ تراکنش در هر ثانیه است و بدیهی است که این مقدار برای انجام همه تراکنش‌های مالی دنیا کفایت نمی‌کند. با توجه به برگشت‌ناپذیر (نهایی) بودن تراکنش‌های ثبت شده روی زنجیره اصلی، از آن برای تصفیۀ مبالغ بالا و دست‌یابی به حداکثر اطمینان از نهایی بودن تراکنش‌ها استفاده می‌شود. اما پرداخت‌های کوچک به امنیت پایین‌تری نیاز دارند و می‌توان آن‌ها را «خارج از زنجیره» و روی لایه‌ای بیرونی که از قوانین اختصاصی خود پیروی می‌کند، اجرا کرد. توسعه لایه‌ای موجب افزایش ظرفیت شبکه و پایین آمدن کارمزدها در پرداخت‌های خرد می‌شود.

توسعه‌دهندگان بیت کوین ترجیح می‌دهند که نوآوری و افزایش ظرفیت شبکه بیت کوین بر روی لایه‌های بیرونی انجام شود تا زنجیره اصلی بیت کوین - که به لایه اول نیز معروف است - از خطرات امنیتی احتمالی که در نتیجه نوآوری‌های نرم‌افزاری پیش می‌آید، مصون باشد.

روش توسعه لایه‌ای مختص به سیستم‌های دیجیتال نیست و در سیستم‌های آنالوگ نیز به کار گرفته می‌شود. به عنوان مثال قبل از منسوخ شدن استاندارد طلا در سیستم بانکداری دنیا، پول نقد کاغذی به عنوان لایه بیرونی طلا که پایه پول بود، به کار گرفته می‌شد.

برنامه سبک

Light Client

به برنامه‌های کاربردی گفته می‌شود که با شبکه بیت کوین تعامل دارند اما زنجیره بلاک را ذخیره نمی‌کنند و در عوض اطلاعات تراکنش‌هایی که برایشان اهمیت دارد را از دیگر نودهای موجود در شبکه دریافت می‌کنند. برای نمونه می‌توان به کیف پول‌های بیت کوین اشاره کرد.

کاربران کیف پول‌های بیت‌کوین از این برنامه‌ها برای اطلاع از موجودی بیت‌کوین و دریافت اطلاعات تکمیلی تراکنش‌های خود استفاده می‌کنند. کیف پول‌هایی که اطلاعات لازم را از دیگر نودهای حاضر در شبکه دریافت می‌کنند از نظر حفظ حریم خصوصی و حذف اعتماد، نسبت به کیف پول‌هایی که به فول نود شخصی کاربران متصل شده‌اند، ضعیف‌تر هستند اما استفاده از آن‌ها آسانتر است و به فضای ذخیره‌سازی دیسک کمتری نیاز دارند.

اکثر کیف پول‌های موبایل و برخی از کیف پول‌های دسکتاپ از این روش استفاده می‌کنند، زیرا اجرای نرم‌افزار نود بیت‌کوین و ذخیره تمام زنجیره بیت‌کوین بر روی برخی از دستگاه‌ها امکان‌پذیر نیست. برنامه‌هایی که برای دریافت اطلاعات مورد نیاز از این روش استفاده می‌کنند، معمولاً به یک سرور مرکزی متصل می‌شوند و اطلاعات را از آن درخواست می‌کنند، اما برخی از آن‌ها به کاربران این اجازه را می‌دهند تا برای حفظ حریم خصوصی و حذف اعتماد به دیگران، به نود شخصی خود متصل شوند.

M

m از n

M-of-N

این اصطلاح شرایط دقیق یک حساب چند امضایی بیت کوین را توصیف می کند که برای انتقال موجودی آن به m امضاء از میان n کلید مجازی که از قبل تعریف شده اند نیاز است. یک آدرس چند امضایی بیت کوین آدرسی است که برای خرج کردن موجودی آن به امضای چندین کلید خصوصی مستقل نیاز است. برخی از کاربران بیت کوین، برای دستیابی به قابلیت اطمینان بالاتر و حفاظت هرچه بهتر از بیت کوین های خود، دارایی خود را به جای قرار دادن در حساب های تک امضایی، آن ها در حساب های چند امضایی قرار می دهند. در این صورت دارایی آن ها با به خطر افتادن تنها کلید موجود، از بین نخواهد رفت. این در حالی است که در حال حاضر اغلب کاربران به روش تک امضایی از بیت کوین های خود نگهداری می کنند.

بیا بید فرض کنیم آوا و بابک و منوچهر می خواهند با هم یک شرکت تأسیس کنند و قصد دارند بخشی از سرمایه شرکت را در قالب بیت کوین و به صورت شراکتی در اختیار داشته باشند. برای اطمینان از اینکه هریک از شرکا به طور جداگانه قادر به انتقال موجودی این حساب نیست، آوا و بابک و منوچهر تصمیم می گیرند این دارایی را در یک حساب چند امضایی بیت کوین قرار دهند. همچنین توافق می کنند که انتقال موجودی این حساب در گرو توافق اکثریت باشد. به این معنی که موجودی این حساب مشترک می تواند در صورت توافق دو نفر از آن ها جابه جا شود. روش کار به این صورت است که هر کدام از آن ها یکی از کلیدهای عمومی شخصی خود را با دیگران به اشتراک می گذارد و یک آدرس بیت کوین از روی آن ها ساخته می شود. به این صورت که برای انتقال موجودی حساب مشترک شرکت، به ۲ امضاء از ۳ امضاء مجازی که در هنگام ساخته شدن آدرس تعریف شده نیاز است. به بیان دیگر حساب این شرکت یک حساب چند امضایی ۲-از-۳ است.

معرف زنجیره بلاک و شبکه اصلی بیت کوین است که به عنوان بیت کوین واقعی شناخته می شود و آن را از دیگر زنجیره ها و شبکه های بیت کوین که اغلب در فرآیند توسعه به منظور آزمون و خطا به خدمت گرفته می شوند و فاقد ارزش مالی هستند، متمایز می کند. هنگامی که فردی به شبکه بیت کوین اشاره می کند در واقع منظور همان شبکه اصلی بیت کوین است که کوین های آن برخلاف کوین های دیگر شبکه های متفرقه مثل شبکه تست و شبکه سیگنت، ارزش پولی دارند.

هریک از این شبکه ها دارای زنجیره بلاک و توکن مخصوص به خود هستند و آدرس هر کدام با یک پیشوند اختصاصی شروع می شود. آدرس های شبکه اصلی بیت کوین با یکی از پیشوندهای ۱، ۳، یا bc1 شروع می شود، در حالی که آدرس های شبکه تست با یکی از پیشوندهای ۲، m یا n، یا tb1 شروع می شود. کوین اختصاصی یک شبکه نباید به یک شبکه دیگر ارسال شود. برای مثال اگر کوین شبکه اصلی بیت کوین به یک آدرس شبکه تست بیت کوین ارسال شود، بیت کوین های با ارزش شبکه اصلی می سوزد و از بین می رود و راهی برای بازیابی آن نخواهد بود. عکس این موضوع نیز صادق است.

تغییر پذیری

Malleability

تغییر پذیری تراکنش یعنی امکان اختصاص چندین شناسه معتبر به یک تراکنش بیت کوین و زمانی اتفاق می افتد که اعمال تغییر در بخشی از یک تراکنش امضاء شده بیت کوین موجب تغییر شناسه آن شود، اما تراکنش مورد نظر همچنان معتبر بماند. از آنجا که شناسه تراکنش در واقع از هاش تراکنش به دست می آید، اعمال هرگونه تغییر در داده یک تراکنش موجب تغییر شناسه آن خواهد شد. این در حالی است که تغییراتی که شناسه تراکنش را تغییر می دهند و موجب بی اعتبار شدن آن می شوند، مایه نگرانی نیستند.

تغییر پذیری تراکنش موجب می شود تا توسعه دهندگان و کاربران قادر نباشند در یک تراکنش جدید به تراکنشی قدیمی که هنوز روی زنجیره بلاک تأیید نشده است، ارجاع دهند. این مشکل به این دلیل به وجود می آید که برای خرج کردن یک خروجی خرج نشده و در زمان وارد کردن آن به

یک تراکنش جدید، می‌بایست به شناسه تراکنشی که این خروجی مورد نظر در آن قرار گرفته ارجاع داده شود. بنابراین اگر امکان تغییر شناسه تراکنش وجود داشته باشد، امکان ارجاع به شناسه قبلی وجود ندارد، زیرا ممکن است در زمان تأیید و ثبت بر روی زنجیره بلاک تغییر کرده باشد و موجب نامعتبر شدن تراکنش جدید شود.

از دو روش می‌توان یک تراکنش را تغییر داد. اولین راه این است که پس از امضاء تراکنش، داده‌های جدیدی به بخش ScriptSig اضافه کنیم. روش دوم این است که داده خود امضاء که در همان بخش قرار دارد را تغییر دهیم.

مشکل تغییرپذیری تراکنش‌های بیت کوین از طریق اجرای سافت فورک سگویت و ارتقاء قوانین پروتکل بیت کوین برطرف، و اجرای نوآوری‌های بیشتری چون شبکه لایتینگ و ارتقاء تپروت بر روی شبکه بیت کوین ممکن شد. سگویت داده امضاء را که بخش تغییرپذیر تراکنش است از بدنه اصلی جدا و به بخش مجزای دیگری به نام شاهد منتقل، و با این کار مشکل تغییرپذیری تراکنش‌های بیت کوین را به کلی برطرف کرد.

Medium of Exchange

واسط معامله

به کالایی گفته می‌شود که امکان تبادل کالاها و خدمات را برای مردم فراهم می‌کند و موجب تسهیل این کار می‌شود. در طول تاریخ چیزهایی مثل صدف‌ها، مهره‌های شیشه‌ای، و طلا به عنوان واسطه معامله مورد استفاده قرار گرفته‌اند اما آن‌ها همه ویژگی‌های لازم برای ایفای نقش یک پول خوب را در اختیار نداشتند. این ویژگی‌ها عبارتند از کمیابی، دوام، قابلیت حمل، تعویض‌پذیری، و بخش‌پذیری.

امروزه پول‌های فیات رایج‌ترین ابزار پرداخت در معاملات مردم جهان هستند زیرا به‌طور گسترده‌ای در سراسر جهان مورد پذیرش قرار می‌گیرند. بیت کوین در سال ۲۰۲۱ و بر اساس قانونی که به «قانون بیت کوین» مشهور است در کشور ال‌سالوادور و در کنار دلار آمریکا به عنوان پول قانونی پذیرفته شد و با افزایش نقدشوندگی آن پتانسیل تبدیل شدن به ابزار پرداخت در معاملات جهانی را

در مقیاس گسترده‌تری پیدا خواهد کرد.

مم پول

Mempool

هریک از نودهای حاضر در شبکه، تراکنش‌هایی که هنوز تأیید نشده‌اند و در صف انتظار برای وارد شدن به بلاک‌ها توسط ماینرها هستند را در پایگاه داده کوچکی به نام مم پول نگه‌داری می‌کند. این تراکنش‌ها پس از تأیید و وارد شدن به زنجیره بلاک، از مم پول حذف می‌شوند. نودهای شبکه تراکنش‌های مم پول خود را از طریق شبکه همتا-به-همتای بیت کوین دست‌به‌دست، و آن‌ها را با یکدیگر به اشتراک می‌گذارند.

برای پایین نگه‌داشتن منابع سخت‌افزاری مورد نیاز برای راه‌اندازی یک نود، که ارتباط مستقیمی با غیرمتمرکز ماندن شبکه بیت کوین دارد، سائز این پایگاه داده در حالت پیش‌فرض روی ۳۰۰ مگابایت تنظیم شده اما هر شخص قادر است این مقدار را برای نود خود تغییر دهد، بنابراین مم پول در نودهای مختلف شبکه ممکن است حاوی تراکنش‌های مختلفی باشند.

سافت فورک فعال‌سازی شده توسط

Miner-Activated Soft Fork

ماینرها (ام‌ای‌اس‌اف)

(MASF)

سافت فورک به اعمال تغییراتی در قوانین پروتکل گفته می‌شود که در صورت حمایت ماینرها، ایجاد ویژگی‌پس‌اسازگاری در آن‌ها ممکن می‌شود و نیازی به به‌روزرسانی همه نودهای حاضر در شبکه نخواهد بود. حال اگر این سافت فورک توسط ماینرهایی که بلاک‌های جدید را بر اساس قوانین جدید می‌سازند اعمال شود، به آن سافت فورک فعال شده توسط ماینرها (MASF) گفته می‌شود. بدین صورت که ماینرها با اعلام حمایت خود از قوانین جدید، در فرآیند به‌روزرسانی قوانین پروتکل شبکه مشارکت می‌کنند. ماینرها فقط در صورتی مجاز به ساختن بلاک‌ها بر اساس قوانین جدید هستند که اکثریت قریب به اتفاق آن‌ها (یا به عبارت دیگر بیشتر از ۹۰ درصد میزان هش)، از اعمال قوانین جدید پشتیبانی کرده باشند.

ماینها یکی از اعضای مهم شبکه بیت کوین هستند زیرا تراکنش‌ها را پردازش می‌کنند و بلاک‌ها را می‌سازند، اما قوانین شبکه بیت کوین توسط آن‌ها تعیین نمی‌شود. اگر ماینها قوانین پروتکل را بدون اجماع تغییر دهند و بلاک‌ها را بر اساس قوانینی که مورد توافق نودهای شبکه نیست بسازند، این بلاک‌ها از نظر شبکه مردود هستند و همه هزینه‌ای که برای ساختن آن‌ها صرف شده به هدر می‌رود و آن‌ها را در معرض ضررهای مالی جدی قرار خواهد داد.

استخراج

Mining

به فرآیند ساخت بلاک‌های جدید و اضافه کردن آن به زنجیره بلاک استخراج گفته می‌شود. ابتدا ماینها تعدادی از تراکنش‌های تأیید نشده را از میان تراکنش‌های واقع در مم‌پول که در انتظار تأیید هستند انتخاب، و یک بلاک می‌سازند. این مرحله از کار نسبتاً ساده است. در مرحله بعد ماینها سعی می‌کنند تا عدد معتبر اثبات کار را برای این بلاک جدید پیدا کنند. این جستجو درواقع بر پایه حدس و گمان است و انرژی بسیار زیادی صرف می‌کند.

ماینها پس از یافتن عدد اثبات کار و اطمینان از معتبر بودن بلاک ساخته شده، آن را به شبکه ارسال می‌کنند. بیت‌کوین‌های جدیدی که به آن‌ها یارانه ساخت بلاک گفته می‌شود نیز از طریق این فرآیند و به‌منظور جبران تلاش‌های ماینها برای یافتن یک بلاک معتبر خلق می‌شوند. این یارانه ماینها را قادر می‌سازد تا هزینه پیدا کردن یک بلاک معتبر که مستلزم صرف انرژی بسیار زیادی است را پرداخت کنند.

ماینها برای ساخت یک بلاک معتبر هیچ راهی بهتر از حدس زدن عدد اثبات کار و بررسی اعتبار آن ندارند، بنابراین سعی می‌کنند تا در کمترین زمان و با صرف کمترین انرژی ممکن، حدس‌های بیشتری بزنند. به تعداد همه حدس‌هایی که یک ماینر می‌تواند برای ساخت یک بلاک معتبر بزند، میزان هَش گفته می‌شود که با واحد هَش بر ثانیه اندازه‌گیری می‌شود. نرخ هَش تجمعی همه ماینرهای مشغول در شبکه بیت‌کوین معیار مهمی برای تعیین امنیت این شبکه است، زیرا نشان می‌دهد که یک مهاجم برای اجرای حمله ۵۱ درصدی به چه میزان هَش نیاز دارد.

صنعت استخراج به دلایل متعددی چون هزینه‌های انرژی، جذب سرمایه‌گذاری، و پیچیدگی‌های فنی، در مقیاس بزرگ بهینه‌تر است. استخرهای استخراج به ماینرهای خرد این اجازه را می‌دهند تا بازدهی خود را افزایش، و به‌جای تلاش برای به‌دست آوردن پاداش‌های بسیار بالا اما نادر، ریسک خود را با کسب پاداش‌های کوچک اما مستمر و قابل پیش‌بینی، کاهش دهند. هنگامی که یکی از اعضای یک استخر استخراج بلاک معتبری را پیدا می‌کند، پاداش کسب شده میان دیگر اعضای استخر و بر اساس میزان هاش هریک از آن‌ها تقسیم می‌شود. گردانندگان استخرهای استخراج نیز معمولاً بابت برقراری هماهنگی میان اعضاء، درصدی از این پاداش را به‌عنوان کارمزد برای خود در نظر می‌گیرند.

سرویس میکس

Mixing

یک سرویس میکس که با نام میکسر یا تامبلر نیز شناخته می‌شود، کوین‌های افراد را به امانت می‌گیرد و کوین‌های دیگری را پس از کسر کارمزد به آن‌ها بازمی‌گرداند. اگر این کار به‌درستی انجام شود به‌طور موثری قادر به پنهان کردن مالکیت صاحبان بیت کوین‌های دریافتی خواهد بود.

برخی از سرویس‌های میکسر با مشکلات حقوقی و اتهاماتی چون پول‌شویی مواجه، و در نهایت تعطیل شده‌اند. زیرا میکسرها برخلاف سرویس‌های کوین‌جوین، امانی هستند و اختیار دارایی کاربران در زمان اجرای فرآیند میکس در اختیار آن‌ها است.

کلمات بازیابی (یادآوری)

Mnemonic

کلمات بازیابی، فهرستی مشتمل بر ۱۲ تا ۲۴ کلمه است که برای پشتیبان‌گیری از یک کیف پول بیت کوین مورد استفاده قرار می‌گیرد. این فهرست درواقع نماینده داده‌ای است که می‌توان با در اختیار داشتن آن کلیدهای یک کیف پول سلسله‌مراتبی قطعی را تولید کرد.

کلمات بازیابی بر اساس بیپ-۳۹ در پروتکل بیت کوین به عنوان استاندارد تعریف شده و اکثر کیف پول‌های بیت کوین از آن پشتیبانی می‌کنند. اکثر کیف پول‌ها همچنین به کاربران اجازه می‌دهند تا به منظور افزایش امنیت، کلمات دلخواهی که با عنوان پسفریز شناخته می‌شود را به انتهای کلمات بازیابی اضافه کنند.

کلمات بازیابی از میان ۲۰۴۸ کلمه انتخاب می‌شوند و کلمه آخر نیز برای افزایش قابلیت اطمینان این روش بازیابی کلید خصوصی، به عنوان یک جمع‌آزمای عمل می‌کند. با توجه به امکان انتخاب کلمات بازیابی از میان یک لیست ۲۰۴۸ کلمه‌ای، احتمال حدس زدن فهرست کلمات بازیابی ۲۴ تا ۱ دیگران، ۱ در 2048^{24} یا $10^{79} \times 2,96$ است.

چند امضایی

Multisig

اغلب تراکنش‌های بیت کوین، آن را به آدرسی ارسال می‌کنند که می‌توان با در اختیار داشتن تنها یک کلید خصوصی و تولید یک امضای دیجیتالی آن را خرج یا به آدرس دیگری منتقل کرد. با این حال امکان ارسال بیت کوین به آدرسی که برای خرج کردن آن به چندین امضاء که توسط کلیدهای خصوصی جداگانه‌ای تولید شده‌اند نیز وجود دارد. به این ترتیب موجودی بیت کوین این آدرس می‌تواند به طور مشترک توسط یک خانواده، شرکای تجاری، هیئت‌مدیره یک شرکت، یا هر گروه دیگری کنترل شود.

یک حساب چند امضایی اغلب به صورت m از n تعریف می‌شود که از n کلید عمومی که از قبل تعریف شده حداقل به m امضاء برای جابه‌جا کردن موجودی آن نیاز است. به عنوان مثال در یک حساب چند امضایی «۲ از ۳»، سه کلید عمومی تعریف می‌شود و امضاء دو کلید خصوصی از این ۳ کلید عمومی برای نقل و انتقال موجودی این حساب کافی است.

برای تولید آدرس‌های بیت کوین در یک حساب چند امضایی می‌توان از استاندارد (P2SH) استفاده کرد که در سال ۲۰۱۲ توسط سافت فورک بیپ-۱۶ معرفی شد و آدرس‌های آن با عدد ۳ شروع می‌شوند، یا از استاندارد (P2WSH) که در سال ۲۰۱۷ توسط سافت فورک سگویت معرفی شد که در

این صورت آدرس‌های آن با bc1q شروع می‌شوند، یا از استاندارد (P2TR) که در سال ۲۰۲۱ میلادی توسط سافت فورک تپروت معرفی شد و آدرس‌های آن با bc1p شروع می‌شوند.

میوسینگ

MuSig

پروتکلی است که با استفاده از ترکیب کلیدهای عمومی و همچنین امضاهای شنور، کلیدهای عمومی و امضاهای دیجیتالی مورد نیاز برای تپروت را تولید می‌کند. خرج کردن از یک حساب چند امضایی تپروت هیچ تفاوتی با خرج کردن بیت کوین از یک حساب تک امضایی تپروت ندارد، زیرا می‌توان با استفاده از میوسینگ کلیدهای عمومی افراد ذینفع در یک حساب چند امضایی را با یکدیگر ترکیب، و یک کلید عمومی تولید کرد که نماینده همه آنها است. صاحبان این حساب چند امضایی برخلاف روش‌های قبلی، در هنگام خرج کردن موجودی این حساب مجبور به فاش کردن کلیدهای عمومی خود نیستند. در عوض آنها به‌طور جمعی و با استفاده از میوسینگ یک امضای معتبر برای کلید عمومی که قبلاً ایجاد کرده بودند، تولید می‌کنند. در روش‌های P2SH و P2WSH امضاها و کلیدهای عمومی هریک از افراد حاضر در یک حساب چند امضایی فاش، و بر روی زنجیره بلاک بیت کوین برای همیشه ثبت می‌شود. این مسأله گذشته از پیامدهای ناخواسته‌ای که روی حریم خصوصی کاربران دارد، موجب اشغال فضای بلاک نیز می‌شود.

Bitcoin Node

نود (گره) بیت کوین

به هریک از اعضاء شبکه بیت کوین که با دیگر نودهای حاضر در شبکه همتا-به-همتا بیت کوین در ارتباط است، یک نود یا گره گفته می‌شود. نود بیت کوین درواقع کامپیوتری است که یکی از نرم‌افزارهای پیاده‌سازی بیت کوین را اجرا، و همه یا بخشی از زنجیره بلاک را ذخیره می‌کند. نودها، بلاک‌ها و همچنین تراکنش‌هایی که در مم‌پول آن‌ها قرار دارد را اعتبارسنجی، و بر بستر یک شبکه همتا-به-همتا و غیرمتمرکز، با یکدیگر دست‌به‌دست می‌کنند. اجماع روی شبکه بیت کوین تنها زمانی رخ می‌دهد که نرم‌افزار نودهای شبکه با یکدیگر سازگار باشد یا به بیان دیگر مجموعه قوانین مشترکی را بر روی شبکه اعمال کنند.

به‌منظور حفظ حریم خصوصی مالی اغلب پیشنهاد می‌شود که کاربران بیت کوین کیف پول‌های خود را به نود شخصی‌شان متصل کنند و برای دریافت اطلاعات تراکنش‌های خصوصی و موجودی کیف پول، به نودهای دیگران اعتماد نکنند. از وظایف مهم نودهای شبکه همچنین می‌توان به حفاظت از قوانین پروتکل و بالا بردن قابلیت اطمینان شبکه اشاره کرد.

Non-Custodial

غیرامانی (غیرحضانتي)

به روشی گفته می‌شود که در آن کنترل کلیدهای خصوصی کاربران در اختیار شخص آن‌ها باشد و هیچ شخص یا نهاد دیگری به کلیدهای خصوصی آن‌ها دسترسی نداشته باشد. تحت اختیار داشتن کلیدهای خصوصی خطر سانسور، مصادره، و به خطر افتادن حریم خصوصی مالی کاربران بیت کوین را از جانب حکومت‌های محلی یا نهادهایی که از کلیدهای خصوصی کاربران به‌صورت امانی نگهداری می‌کنند از بین می‌برد.

با این حال، یادآوری این نکته ضروری است که در اختیار گرفتن کنترل کلیدهای خصوصی

بیت کوین به صورت غیرامانی، مسئولیت‌های مهمی با خود به همراه می‌آورد. اگر شما کنترل بیت کوین خود را شخصا بر عهده داشته باشید اما دسترسی به کلیدهای خصوصی خود را به هر دلیلی از دست دهید، هیچ کس قادر نیست به شما کمک کند و آن‌ها برای همیشه از دست خواهند رفت. کاربران بیت کوین اغلب روش‌هایی چون نگهداری از نسخه‌های پشتیبان در مکان‌های مختلف و نگهداری از بیت کوین به روش چند امضایی را برای جلوگیری از از دست رفتن دارایی خود به خدمت می‌گیرند.

نانس

Nonce

این کلمه در انگلیسی مخفف «عدد یک‌بار مصرف»، و یکی از متغیرهایی است که ماینرها در روند ساخت بلاک و پیدا کردن یک عدد اثبات کار معتبر از آن استفاده می‌کنند. روند کار به این صورت است که ماینرها برای تولید هش‌های متفاوت اما معتبر از یک بلاک، متغیرهای مجاز را تغییر می‌دهند و یکی از این متغیرهای مجاز عدد نانس است. با توجه به قرار گرفتن این متغیر در سربرگ بلاک، می‌توان به سادگی و با تغییر آن، هش‌های متفاوتی از یک بلاک مورد نظر تولید کرد. پس از پیدا شدن عدد اثبات کار برای یک بلاک که اغلب با صرف زمان و انرژی همراه است، همه نودهای حاضر در شبکه با توجه به خصوصیات عملگرهای هش، قادرند در زمان بسیار کوتاهی به اعتبارسنجی بلاک مورد نظر بپردازند و در صورت معتبر بودن آن را در شبکه همتا-به-همتای بیت کوین دست‌به‌دست کنند.

0

خارج از زنجیره

Off-Chain

اصطلاحی است که برای توصیف هرگونه داده‌ای که بر روی زنجیرهٔ بلاک بیت کوین ثبت نشده باشد، به کار می‌رود. داده‌های خارج از زنجیره شامل تراکنش‌های امضاء شدهٔ بیت کوین که هنوز به شبکهٔ بیت کوین ارسال نشده‌اند و همچنین داده‌هایی که روی شبکهٔ لایتینگ یا دیگر زنجیره‌های جانبی قرار دارند نیز می‌شود.

روی زنجیره

On-Chain

اصطلاحی است که برای توصیف هرگونه داده‌ای که بر روی زنجیرهٔ بلاک بیت کوین ثبت شده است، به کار می‌رود. از داده‌های ذخیره شده بر روی زنجیره می‌توان به بلاک‌ها و تراکنش‌ها اشاره کرد.

کدهای عملیاتی (آپ‌کُد)

Opcode

به دستورات پایه‌ای گفته می‌شود که در برخی از زبان‌های برنامه‌نویسی تعریف شده‌اند. زبان برنامه‌نویسی بیت کوین که اسکریپت نام دارد نیز دارای مجموعه‌ای از کدهای عملیاتی خاص خود است. این کدهای عملیاتی شماره‌گذاری شده‌اند و هر کدام عملکرد محدود و از پیش تعیین‌شده‌ای دارند. در زبان اسکریپت‌نویسی بیت کوین، یک اسکریپت از ترکیب کدهای عملیاتی و داده‌های اضافی مانند آدرس‌ها، کلیدهای عمومی، و امضاها ساخته می‌شود.

برای نمونه می‌توان به P2PKH که یکی از رایج‌ترین انواع اسکریپت‌های بیت کوین است، اشاره کرد که با ترکیب ۴ کُد عملیاتی و هَش یک کلید عمومی ساخته می‌شود. این اسکریپت نوعی از یک ScriptPubKey است که برای قفل کردن بیت کوین از آن استفاده می‌شود و فقط در صورت فراهم

آوردن کلید عمومی و امضاء معتبر می‌توان آن را باز، و بیت‌کوین‌های داخلش را خرج، یا به فرد دیگری منتقل کرد.

نرم‌افزارِ متنِ باز

Open-source software (OSS)

نرم‌افزار متن باز نرم‌افزاری است که سورسِ کُد آن به صورت عمومی منتشر می‌شود. سورس کُد، بخشی از نرم‌افزار است که برنامه‌نویسان با تغییر آن، نحوه رفتار برنامه یا اپلیکیشن را کنترل می‌کنند اما اکثر کاربران هرگز برخوردی با آن نخواهند داشت. برنامه‌نویسانی که به سورس کد یک نرم‌افزار دسترسی دارند قادرند با تغییر یا اضافه کردن قسمت‌های جدید، طرز کار آن را به نحوی که می‌خواهند تغییر دهند یا بخش‌هایی که درست کار نمی‌کنند را اصلاح کنند. شرایط مشاهده، اعمال تغییرات، و از همه مهمتر بازنشر یک نرم‌افزارِ متن باز بستگی به مجوز آن دارد.

همه نرم‌افزارهای متن باز، آزاد نیستند. نرم‌افزار آزاد در زبان انگلیسی با عنوان Free software شناخته می‌شود که در آن کلمه Free به معنی «آزاد» است، نه «رایگان». ریچارد استالمن، بنیانگذار پروژه GNU نرم‌افزار آزاد را به این شکل تعریف می‌کند:

«نرم‌افزار آزاد یعنی احترام به آزادی کاربران و جوامعی که از آن استفاده می‌کنند. نرم‌افزار آزاد نرم‌افزاری است که کاربران قادرند آزادانه آن را اجرا کنند، تکثیر و منتشر کنند، سورس کد آن را مطالعه کنند، و با اعمال تغییرات آن را بهبود بخشند. بنابراین نرم‌افزار آزاد یعنی نرم‌افزاری که آزاد است و منظور از free، مجانی بودن آن نیست. برای درک این مفهوم باید مفهوم آزادی در «آزادی بیان» را در نظر بگیرید، نه «ساندیس مجانی». برای جلوگیری از سوءبرداشت در مفهوم آزادی، برخی اوقات بجای free software از عبارت libre software استفاده می‌شود.»

پروژه‌های زیر متن باز هستند، اما در آن‌ها اجازه بازنشر به کاربران داده نشده یا محدودیت‌هایی برای آن در نظر گرفته شده است، بنابراین در گروه نرم‌افزار آزاد قرار نمی‌گیرند:

- Apple macOS's kernel (Darwin)
- Coldcard firmware
- Umbrel

از پروژه‌های آزاد و متن باز می‌توان به پروژه‌های زیر اشاره کرد:

- GNU/Linux
- Bitcoin Core
- Wallet Projects:
 - Electrum Wallet
 - Samurai Wallet
 - Sparrow Wallet
 - BlueWallet
- LibreOffice
- Mozilla Firefox

بلاک بلا تکلیف (بلاک یتیم)

Orphan Block

پارامتر سختی شبکه به صورتی در شبکه بیت کوین تنظیم می‌شود که به طور میانگین هر ۱۰ دقیقه یک بلاک ساخته شود، اما گاهی اوقات پیش می‌آید که دو ماینر به صورت همزمان موفق به ساخت بلاکی می‌شوند که شماره بلاک هر دوی آن‌ها در طول زنجیره با یکدیگر برابر است. یکی از این دو بلاک که تقریباً به صورت همزمان در شبکه همتا-به-همتا بین نودهای حاضر در شبکه دست‌به‌دست می‌شوند زودتر به نیمی از نودهای شبکه می‌رسد، در حالی که نیمه دیگر شبکه بلاک دیگر را زودتر دریافت می‌کند. به بیان دیگر نودهای شبکه به جای یک بلاک، دو بلاک را پشت سر هم و با اندکی تأخیر از شبکه دریافت می‌کنند اما با توجه به اینکه هر دو بلاک معتبر هستند، هر دو را نگه می‌دارند. در این صورت دو زنجیره معتبر خواهیم داشت و این موضوع تا زمانی که ماینر بلاک بعدی، بلاک تازه ساخته شده خود را بر روی یکی از این زنجیره‌ها قرار دهد، ادامه خواهد داشت. در نهایت یکی از زنجیره‌ها طولانی‌تر می‌شود و نودهای شبکه، زنجیره کوتاه‌تر را رها خواهند کرد. به بلاک‌هایی که در زنجیره کوتاه‌تر وجود دارند و از سوی ماینرها رها می‌شوند، در اصطلاح بلاک‌های بلا تکلیف، یا یتیم گفته می‌شود. طول زنجیره بلاک‌های بلا تکلیف اغلب بیشتر از یک بلاک نمی‌شود، اما از نظر تئوری هیچ‌گونه محدودیتی در شبکه بیت کوین برای طول زنجیره بلاک‌های بلا تکلیف وجود ندارد.

هدف توسعه‌دهندگان، و همچنین مطالبه‌ماینرها این است که تعداد بلاک‌های بلاکلیف در شبکه بیت‌کوین به پایین‌ترین تعداد ممکن برسد، زیرا این رویداد موجب از دست رفتن پاداش ساخت بلاک برای ماینرها می‌شود و ضررهای مالی سنگینی در پی دارد. برای رسیدن به این هدف باید بلاک‌ها تا حد امکان با بیشترین سرعت بین نودهای شبکه منتشر شوند و در کوتاه‌ترین زمان به همه آنها برسند. یکی از دلایل محدود بودن سائز یا وزن بلاک‌ها در شبکه بیت‌کوین نیز همین است.

P

Partially Signed Bitcoin Transaction (PSBT)

تراکنشی که امضاء آن ناقص است

استانداردی است که نقل و انتقال تراکنش‌هایی که به‌طور کامل امضاء نشده‌اند را برای کاربران تسهیل می‌کند و اغلب در حساب‌های چند امضایی، پرداخت پی‌جوین، یا سرویس‌های کوین‌جوین که ایجاد یک تراکنش مشترک به تعامل افراد مختلف نیازمند است به کار گرفته می‌شود.

کاربران با به‌کارگیری روش PSBT قادرند در مرحله اول ساختار تراکنش مورد نظرشان را با استفاده از کیف پولی که به اینترنت دسترسی، و از موجودی و خروجی‌های خرج‌نشده آن‌ها اطلاع دارد، بسازند. این تراکنش بدون امضاء معتبر نیست، بنابراین در مرحله دوم کاربر آن را به کلداستوریج خود منتقل و امضاء را به آن اضافه می‌کند. این تراکنش اکنون کامل است و می‌توان آن را به شبکه بیت کوین ارسال کرد، اما کلداستوریج برای حفظ امنیت کلید خصوصی کاربر به اینترنت دسترسی ندارد. در مرحله سوم کاربر مجدداً تراکنش را به کیف پول آنلاین منتقل و آن را به شبکه بیت کوین ارسال می‌کند.

همچنین می‌توان از این روش برای ساخت یک تراکنش چند امضایی استفاده کرد. به عنوان مثال فرض کنید آوا و بابک و منوچهر با هم یک حساب چند امضایی بیت کوین داشته باشند که برای نقل و انتقال آن به ۲ امضا از ۳ امضاء تعریف شده نیاز باشد. به‌کارگیری استاندارد PSBT روند ساخت و تهیه امضاهای لازم برای این تراکنش موردنظر را برای آن‌ها تسهیل می‌کند.

استاندارد PSBT همچنین موجب ایجاد هماهنگی هرچه بیشتر بین نرم‌افزارهای مختلف کیف پول می‌شود و باعث می‌شود کیف پول‌های مختلف قادر به تعامل با یکدیگر باشند. اهمیت این موضوع در مواقعی که کلیدهای خصوصی برای امنیت هرچه بیشتر روی دستگاه‌های آفلاین (کلداستوریج) نگهداری می‌شوند بیشتر نمایان می‌شود. کیف پول‌های نرم‌افزاری و سخت‌افزاری که در طول

سال‌های اخیر به بازار عرضه شده‌اند برای نقل و انتقال فایل تراکنشی که به صورت PSBT تهیه شده از دوربین و کُدهای QR استفاده می‌کنند.

جزئیات نسخه صفر این استاندارد در پیشنهاد بهبود بیت کوین شماره ۱۷۴ و نسخه دوم آن در پیشنهاد شماره ۳۷۰ تعریف شده است.

پرداخت تعاملی (پی‌جوین)

PayJoin (P2EP)

نوع خاصی از تراکنش‌های بیت کوین است که در آن فرستنده و گیرنده برای بی اثر کردن ترفند مالک مشترک ورودی‌های تراکنش با یکدیگر تعامل، و با مشارکت هم تراکنشی می‌سازند که موجب حفظ حریم خصوصی آن‌ها شود.

ترفند مالک مشترک ورودی‌های تراکنش یکی از متداول‌ترین روش‌های به کار گرفته شده در سیستم‌های پایش زنجیره است و فرض را بر این می‌گذارد که همه ورودی‌های وارد شده به یک تراکنش مشخص توسط یک نفر یا یک نهاد امضاء شده‌اند. این سیستم‌ها بر پایه این فرض و به کمک اطلاعاتی که از طریق صرافی‌ها و داده‌های احراز هویت کاربران در دست دارند، اقدام به شناسایی افراد می‌کنند. این ترفند تا قبل از به وجود آمدن پروتکل‌هایی مانند پی‌جوین و کوین‌جوین تا حد زیادی دقیق و قابل استناد بوده، زیرا میزان استفاده از تراکنش‌های چندامضایی در شبکه بیت کوین کم است.

پی‌جوین در واقع پروتکلی است که به دو کاربر بیت کوین اجازه می‌دهد تا با تعامل با یکدیگر تراکنشی بسازند که با بی اثر کردن برخی از ترفندهای پایش زنجیره، از حریم خصوصی آن‌ها حفاظت کند. فرستنده و دریافت‌کننده بیت کوین در حین ساخت تراکنش و طبق پروتکل پی‌جوین و روی یک بستر امن با یکدیگر ارتباط برقرار می‌کنند و اطلاعات مربوط به کوین‌هایی (UTXO) که قصد دارند در ورودی این تراکنش به اشتراک بگذارند را با یکدیگر مبادله می‌کنند. این پروتکل برای سهولت در انتقال تراکنش بین طرفین، از استاندارد تراکنش‌هایی که به صورت ناقص امضا شده‌اند (PSBT) استفاده می‌کند. یک تراکنش پی‌جوین از نظر ظاهری هیچ تفاوتی با دیگر

تراکنش‌های بیت‌کوین ندارد، با این تفاوت که همواره بیشتر از یک ورودی خواهد داشت.

همتا-به-همتا

Peer-to-Peer (P2P)

شبکه همتا-به-همتا یک پروتکل ارتباطی برای اتصال کامپیوترها با یکدیگر و تشکیل یک شبکه کامپیوتری است. هریک از اعضای حاضر در یک شبکه همتا-به-همتا - که به نود (گره) نیز شناخته می‌شوند،- قادرند داده‌های خود را به صورت بدون واسطه و غیرمتمرکز با یکدیگر به اشتراک بگذارند. در یک شبکه همتا-به-همتا تفاوتی میان نودهای تشکیل‌دهنده شبکه وجود ندارد (وجه تسمیه نام این شبکه، ارتباط مستقیم و بدون واسطه آن‌ها با یکدیگر است)، و برای ارتباط با یکدیگر به کسب مجوز از هیچ فرد یا نهاد مرکزی نیاز نیست. متوقف کردن شبکه‌های همتا-به-همتا بسیار دشوار و تقریباً محال است. یک نمونه بسیار معروف از این معماری شبکه «بیت‌تورنت» است. این شبکه علیرغم مشکلات حقوقی که شرکت‌های بزرگ فیلم‌سازی و تهیه‌کنندگان موسیقی در دهه گذشته برای آن به وجود آورده‌اند، و تلاش‌های جدی که از جانب مخالفان این شبکه برای متوقف کردن آن صورت گرفته است، همچنان به کار خود ادامه می‌دهد و راهی برای از کار انداختن آن وجود ندارد.

شبکه بیت‌کوین نیز بر پایه معماری شبکه‌های همتا-به-همتا طراحی و پیاده‌سازی شده و نودهای شبکه به صورت مستقیم با یکدیگر در ارتباط هستند و تراکنش‌ها و بلاک‌ها را به صورت غیرمتمرکز در شبکه دست‌به‌دست می‌کنند. در شبکه بیت‌کوین ارسال و دریافت بیت‌کوین نیز به صورت همتا-به-همتا صورت می‌پذیرد. یک تراکنش بیت‌کوین، مقدار مشخصی بیت‌کوین را به صورت مستقیم و بدون واسطه به فرد دریافت‌کننده منتقل می‌کند و ماینرها که وظیفه پردازش تراکنش‌ها را برعهده دارند، هرگز قادر نخواهند بود دارایی کاربران را در حین ساخت بلاک‌های جدید در اختیار بگیرند یا آن را سرقت کنند.

همانطور که پیشتر اشاره شد، شبکه‌های همتا-به-همتا در برابر سانسور و خراب‌کاری مقاوم هستند و شبکه بیت‌کوین نیز یکی از نمونه‌های بارز آن است. ده‌ها هزار نود (گره) در شبکه بیت‌کوین،

نرم افزار بیت کوین را برای اعتبارسنجی بلاک ها و تراکنش ها اجرا، و به غیر متمرکز ماندن آن کمک می کند.

یک سیستم مالی که به صورت همتا-به-همتا کار می کند اساساً با خدمات مالی مثل حواله های بین بانکی، جابجایی پول به صورت کارت به کارت، و کارت خوان های مستقر در فروشگاه ها که توسط نهادهای مالی متمرکز ارائه می شود، متفاوت است. بانک ها و دولت ها می توانند در روند جابجایی پول کاربران در این سیستم ها دخالت کنند، آن را به تعویق اندازند، سانسور، یا حتی متوقف کنند. در زمان نگارش این مطلب هر فرد ایرانی می تواند در طول شبانه روز ۲۰۰ هزار تومان (کمتر از ۱۰ دلار آمریکا) از دستگاه های خودپرداز پول نقد دریافت کند و برای جابجایی پول در شبکه بانکی نیز محدودیت های سخت گیرانه ای وجود دارد. محدودیت های دولتی در کنار تحریم های بین المللی فرآیند نقل و انتقال پول را برای شهروندان کشورهایی چون ایران بسیار گران می کند و بر روی زندگی آنان اثر مستقیم دارد.

پیوند ارزش (پگ)

Peg

هنگامی که ارزش یک دارایی به صورت مستقیم به ارزش دارایی دیگری وابسته شود، اصطلاحاً می گوئیم ارزش کالای اول به ارزش کالای دوم پیوند خورده است. به عنوان نمونه می توان به پول های رایج در کشورهای مختلف جهان اشاره کرد که ارزش پول شان را با نسبتی که عمدتاً توسط بانک های مرکزی تعیین می شود، به ارزش دلار آمریکا به عنوان پول مرجع دنیا تعیین می کنند. تعیین، و تلاش برای تثبیت ارزش پول ملی کشورها به منظور افزایش اعتماد سرمایه گذاران انجام می پذیرد.

این مفهوم در حوزه بیت کوین در زنجیره های جانبی موضوعیت پیدا می کند. در این زنجیره ها که به صورت یک راه حل خارج از زنجیره طراحی و اجرا می شوند، عموماً توکن هایی خلق می شوند که ارزش آن ها نسبت به بیت کوین سنجیده می شود و ارزش آن ها به اصطلاح به ارزش بیت کوین پیوند می خورد. برای مثال می توان به زنجیره جانبی لیکوئید اشاره کرد که ارزش توکن آن (L-BTC) نسبت به ارزش بیت کوین به صورت ۱:۱ تعیین شده است.

به داده ورودی به یک عملگر هَش گفته می‌شود، که به منظور محاسبه هَش به آن وارد می‌شود. از آنجا که توابع هَش به کار گرفته شده در حوزه رمزنگاری یک طرفه هستند، با در اختیار داشتن خروجی تابع هَش راهی برای به دست آوردن داده ورودی (پری‌ایمِج) وجود ندارد.

ورودی یک تابع هَش می‌تواند هر نوع داده‌ای باشد. به عنوان مثال، آدرس‌ها در شبکه بیت کوین از روی هَش کلیدهای عمومی ساخته می‌شوند. سربرگ بلاک نیز داده ورودی (پری‌ایمِج) اثبات کار بلاک است که در واقع خود یک هَش است.

کلید خصوصی

Private Key

برای نقل و انتقال یا خرج کردن بیت کوین‌هایی که به یک آدرس بیت کوین واریز شده، می‌بایست کلید خصوصی مرتبط به کلید عمومی که آدرس از روی آن ساخته شده است را در اختیار داشته باشیم، زیرا تولید یک امضاء دیجیتال معتبر فقط با در اختیار داشتن کلید خصوصی میسر است. در حالی که هیچ گونه محدودیتی در انتشار کلیدهای عمومی وجود ندارد، باید کلیدهای خصوصی را در مکانی امن نگهداری کرد، چون هر کس کلیدهای خصوصی را در اختیار داشته باشد قادر به نقل و انتقال بیت کوین‌ها نیز خواهد بود.

کیف پول‌های بیت کوین در واقع شبیه به یک دسته کلید هستند و عموماً وظیفه تولید و مدیریت کلیدهای عمومی و خصوصی، ساخت آدرس‌ها، تولید امضاهای دیجیتال برای تراکنش‌ها، و تا حد امکان نگهداری امن از کلیدهای خصوصی را بر عهده دارند.

کیف پول‌های سخت افزاری برای افزایش ضریب امنیت در نگهداری از کلیدهای خصوصی، آن‌ها را به صورت آفلاین و در محیطی ایزوله نگهداری، و از استاندارد تراکنش‌هایی که به صورت ناقص امضا شده‌اند (PSBT) و همچنین دوربین و QR کدهای برای نقل و انتقال داده‌ها در زمان ساخت تراکنش و تولید امضاء دیجیتال بر روی دستگاه‌های مختلف استفاده می‌کنند.

اثبات صحت و درستی داده‌ها در شبکه بیت کوین از طریق به کارگیری روش اثبات کار انجام می‌پذیرد. ماینرهای بیت کوین باید اثبات کار بلاک ساخته شده خود را در قالب یک هش معتبر به شبکه ارسال کنند تا شبکه آن را به عنوان یک بلاک معتبر بپذیرد. اثبات کار، ماینرها را مجبور به صرف پول و انرژی زیادی برای تولید بلاک‌ها می‌کند، بنابراین آن‌ها تشویق به امانت‌داری می‌شوند و تقلب برای آن‌ها بسیار گران تمام خواهد شد. در حال حاضر روش اثبات کار (PoW) تنها راه حل عملی برای حل مسئله ژنرال‌های بی‌انصاف و توافق روی درستی زنجیره بلاک در یک شبکه غیرمتمرکز مانند شبکه بیت کوین است؛ ویژگی که برای یک سیستم مالی حیاتی به شمار می‌رود.

ماینرها با تولید بلاکی که هش آن کوچکتر از یک عدد تعیین شده است، یک اثبات کار معتبر می‌سازند. خروجی عملگر هش SHA-256 که در استخراج شبکه بیت کوین مورد استفاده قرار می‌گیرد، عددی است که در کدبندی هگزادسیمال ۶۴ کاراکتر دارد و با توجه به خصوصیات عملگرهای هش، تصادفی است. بنابراین ماینرها باید میلیاردها هش را در هر ثانیه تولید کنند تا به صورت تصادفی یک هش که از عدد هدف کوچکتر است، پیدا شود. عدد هدف یا به عبارت دیگر سختی شبکه به صورت خودکار توسط کد بیت کوین تنظیم می‌شود.

هرچه میزان هش با پیوستن ماینرهای بیشتر به شبکه افزایش یابد، عدد هدف کاهش می‌یابد و یافتن یک هش که پایین تر از عدد هدف باشد برای ماینرها دشوارتر خواهد شد. برعکس اگر ماینرها شبکه را ترک کنند و میزان هش کاهش یابد، عدد هدف افزایش پیدا می‌کند تا پیدا کردن یک هش معتبر برای ماینرها آسانتر شود. الگوریتمی در کد بیت کوین وجود دارد که هر ۲۰۱۶ بلاک - تقریباً هر دو هفته - عدد هدف را بازتنظیم می‌کند. این کار برای اطمینان یافتن از روند خلق بیت کوین‌های جدید و تثبیت سیاست پولی بیت کوین انجام می‌شود. برای رسیدن به این هدف می‌بایست به طور میانگین هر ۱۰ دقیقه یک بلاک جدید توسط ماینرها پیدا شود. توجه به این نکته ضروری است که مفهوم «پیدا شدن» بلاک اشاره به تصادفی بودن روند ساخت بلاک‌ها دارد و گاهی اوقات در متون فنی بیت کوین به کار گرفته می‌شود.

پروتکل، به مجموعه قوانینی گفته می‌شود که رفتار یک شبکه را تعریف می‌کند. قوانین پروتکل شبیه به قانون اساسی است و این موضوع در مورد بیت کوین نیز صادق است. نودهایی که نرم‌افزار بیت کوین را اجرا می‌کنند روی شبکه اعمال می‌شود و برای رسیدن به توافق نیازی به اعتماد یا کسب اجازه از یک نهاد مرکزی مانند دادگاه عالی، یا مدیرعامل یک شرکت بزرگ نخواهد بود. پروتکل بیت کوین برای ایجاد یک شبکه پولی همتا-به-همتا، از زنجیره بلاک و روش اجماع بر اساس اثبات کار استفاده می‌کند.

افراد برای حفاظت از هویت واقعی خود از نام مستعار استفاده می‌کنند. همچنین نام مستعار به آن‌ها این اجازه را می‌دهد تا شهرت عمومی خود را از هویت واقعی‌شان جدا کنند. در مورد بیت کوین، افراد قادرند بدون نیاز به احراز هویت در سطح زنجیره بلاک، با استفاده از کلیدهای عمومی اقدام به دریافت بیت کوین کنند. با این حال این به هیچ وجه تضمینی برای آشکار نشدن هویت کاربران بیت کوین نیست، بلکه تنها تضمین می‌کند که کاربران برای تعامل با زنجیره بلاک بیت کوین الزامی به فاش کردن هویت واقعی خود ندارند.

شرکت‌های تجزیه و تحلیل‌کننده زنجیره و دولت‌ها همواره در تلاشند تا هویت واقعی کاربران بیت کوین را شناسایی، و آدرس‌ها و کلیدهای عمومی ثبت شده روی زنجیره بلاک بیت کوین را به هویت واقعی صاحبان‌شان مرتبط کنند. صرافی‌های بیت کوین با در اختیار گذاشتن اطلاعاتی که طبق قوانین شناسایی مشتریان و قوانین ضد پول‌شویی از کاربران و آدرس‌های آنان جمع‌آوری می‌کنند نیز آن‌ها را در راه رسیدن به این هدف کمک می‌کنند. با فاش شدن هویت واقعی صاحب یک آدرس بیت کوین، نام مستعار به کار گرفته شده برای همیشه بی‌فایده خواهد شد.

از این رو فعالان جامعه بیت کوین و حریم خصوصی همواره اثرات مخرب خرید بیت کوین از صرافی‌ها را به کاربران گوشزد می‌کنند و همچنین برای توسعه و در دسترس قرار گرفتن ابزارها و پروتکل‌هایی مانند کوین‌جوین، پی‌جوین، و تاخت‌زدن کوین که موجب حفظ حریم خصوصی

کاربران می‌شوند، تلاش می‌کنند.

کلید عمومی

Public Key

برای ساخت آدرس‌های بیت‌کوین از کلیدهای عمومی استفاده می‌شود. هنگامی که به یک کلید عمومی بیت‌کوین ارسال شود، برای نقل و انتقال یا خرج کردن آن نیاز به امضاء دیجیتال معتبری است که فقط دارنده کلید خصوصی که کلید عمومی مورد نظر از آن مشتق شده قادر به ساخت آن است. می‌توان کلید عمومی را به یک آدرس ایمیل تشبیه کرد، چرا که هرکس قادر است به این آدرس ایمیل ارسال کند، در حالی که تنها صاحب حساب ایمیل است که با در اختیار داشتن کلید خصوصی (اینجا رمز عبور سرویس ایمیل) قادر به دسترسی و خواندن نامه‌های دریافت شده است. بیت‌کوین از سیستم رمزنگاری ای‌سی‌دی‌اس‌ای استفاده می‌کند که می‌توان در آن برای هر کلید خصوصی یک تا چند کلید عمومی متناظر ساخت. منتشر کردن یک کلید عمومی گذشته از مخاطراتی که برای حریم خصوصی صاحب آن به وجود می‌آورد، خطری برای بیت‌کوین‌هایی که به آن ارسال می‌شود در پی نخواهد داشت، در حالی که کلید خصوصی می‌بایست تحت هر شرایطی مخفی و از دسترس دیگران مصون باشد، زیرا دسترسی به کلید خصوصی به معنی در اختیار داشتن بیت‌کوین‌های ارسال شده به کلیدهای عمومی متناظر با آن است.

مفاهیم آدرس و کلید عمومی اغلب به جای یکدیگر مورد استفاده قرار می‌گیرند، اما آدرس‌ها درواقع هَش کلیدهای عمومی هستند و برای سهولت استفاده کاربران از آن‌ها استفاده می‌شود، در حالی که اعتبارسنجی امضاء دیجیتال در یک تراکنش بیت‌کوین با استفاده از کلید عمومی انجام می‌پذیرد.

وظیفه کیف پول‌های بیت‌کوین تولید و مدیریت کلیدهای خصوصی و عمومی کاربران است. یک کیف پول برای انجام این کار ابتدا کلید خصوصی که درواقع یک عدد بسیار بزرگ است را تولید می‌کند. سپس درخت کلیدهای خصوصی و عمومی با استفاده از روش سلسله‌مراتبی و قطعی ساخته می‌شود و در نهایت این آدرس‌های بیت‌کوین هستند که از روی کلیدهای عمومی ساخته، و آماده استفاده کاربران می‌شوند.

Q

کُدِ کیوآر

QR Code

کُدِ کیوآر ابزاری برای ترسیم داده‌های مختلف به صورت گرافیکی است و کارکردی شبیه به بارکُد دارد. یک کُدِ کیوآر می‌تواند نمایانگر آدرس یک سایت، یک آدرس بیت کوین، فاکتور پرداخت شبکه لایت‌نینگ، یا موارد دیگر باشد. یک کُدِ کیوآر اغلب به شکل مربع است و با مربع‌های سیاهی که در سه گوشه آن قرار گرفته‌اند شناسایی می‌شود. کُد‌های کیوآر از مربع‌های سیاه و سفید کوچکتری تشکیل می‌شوند که بر اساس الگویی از پیش تعیین شده در کنار یکدیگر قرار گرفته‌اند.

امروزه می‌توان با به کارگیری از ابزار دوربین اکثر تلفن‌های هوشمند، کُد‌های کیوآر را اسکن و داده آن‌ها را خواند. برای این کار کافی است دوربین تلفن خود را به سمت یکی از این کُد‌ها بگیرید تا داده نهفته در آن برای شما به نمایش درآید.

R

تستِ رگ‌سیون (رِگِ تست)

Regtest

شبکهٔ تستِ رگ‌سیون یک زنجیرهٔ بلاک موازی با زنجیرهٔ بلاک شبکهٔ اصلی بیت‌کوین است که افراد می‌توانند آن را به صورت خصوصی اجرا کنند و قوانین پروتکل بیت‌کوین عیناً بر روی آن نیز اعمال می‌شود. راه‌اندازی شبکهٔ رگ‌تست بسیار آسان است و کوین‌های آن مانند شبکهٔ تست بیت‌کوین از ارزش پولی برخوردار نیستند، بنابراین توسعه‌دهندگان بیت‌کوین اغلب در مرحلهٔ تست و توسعهٔ ایده‌ها و ابزارهای خود، از این شبکه استفاده می‌کنند.

ارتباط با دیگر نودهای شبکهٔ همتا-به-همتای بیت‌کوین در شبکهٔ رگ‌تست محدود، و سختی استخراج بر روی عدد صفر تنظیم شده است. بنابراین کاربر شبکهٔ رگ‌تست قادر است در یک زمان کوتاه هر مقدار بلاک و تراکنش که لازم است را بسازد و این ویژگی روند آزمایش و تست ابزارها و ایده‌ها را برای توسعه‌دهندگان آسان‌تر می‌کند.

بازترتیبِ بلاک‌ها (ری‌اُرگ)

Reorganization (reorg)

بازترتیبِ بلاک‌ها که اغلب به آن ری‌اُرگ گفته می‌شود، زمانی اتفاق می‌افتد که یک (یا در موارد بسیار نادر) چند بلاک به دلیل ایجاد زنجیرهٔ طولانی‌تری - که شامل بلاک‌های موردنظر نمی‌شود، - نامعتبر، و از زنجیرهٔ اصلی حذف شوند. ری‌اُرگ به طور کلی برای شبکهٔ بیت‌کوین رویداد نامطلوبی است اما بیشترین آسیب آن به ماینر بلاک حذف شده می‌رسد، زیرا موجب از دست رفتن پاداش ساخت بلاک مورد نظر می‌شود. دلیل رخ دادن ری‌اُرگ این است که نودهای شبکهٔ بیت‌کوین همواره بلندترین زنجیره‌ای که اثباتِ کارِ تجمعی بیشتری داشته باشد را به عنوان زنجیرهٔ معتبر قبول می‌کنند.

تصور کنید ۵۰۰ بلاک در طول زنجیرهٔ بیت‌کوین وجود داشته باشد. یک ماینر بلاک شمارهٔ ۵۰۱ را

نودهای حاضر در شبکه همتا-به-همتا بیت کوین در سطح شبکه از قوانین و مدل امنیتی پروتکل بیت کوین (یعنی اثبات کار) محافظت می کنند، اما برای جلوگیری از رخداد ری آرگ که بیشترین ضرر را به ماینرها می رساند، دو مقوله تمرکززدایی از صنعت استخراج در مقیاس کلان و همچنین بالا بودن میزان هش در شبکه بسیار حیاتی هستند. هرچه صنعت استخراج بیت کوین غیرمتمرکزتر باشد، هماهنگ شدن ماینرهایی که در کشورها و قاره های مختلف قرار دارند عملاً غیرممکن تر خواهد شد، زیرا انگیزه های این بازیگران که در نقاط متفاوت و تحت نظارت قوانین مختلف به استخراج مشغول هستند لزوماً با یکدیگر تطابق ندارد. از طرف دیگر هرچه میزان هش شبکه بالاتر باشد، امکان اجرای حمله ۵۱ درصد و ایجاد یک زنجیره جایگزین (ری آرگ) دشوارتر خواهد بود.

جایگزین کردن توسط کارمزد (آربی اف) Replace-By-Fee (RBF)

آربی اف یکی از ویژگی های اختیاری تراکنش های بیت کوین است که فعال کردن یا نکردن آن به تصمیم فردی که تراکنش را می سازد بستگی دارد. اگر ویژگی آر بی اف برای یک تراکنش بیت کوین فعال باشد، این بدان معنی است که فرد ارسال کننده بیت کوین اجازه دارد تراکنش مورد نظر را با تراکنش دیگری که کارمزد تراکنش بالاتری به ماینرها می پردازد جایگزین کند. این سازوکار به کاربران اجازه می دهد در صورت بالا رفتن غیرمنتظره تعداد تراکنش هایی که در مempool در انتظار تأیید قرار دارند، عکس العمل نشان داده و به قصد پایین آمدن زمان انتظار برای تأیید تراکنش، کارمزد آن را بیشتر کنند. ممکن است کاربری یک تراکنش با کارمزد پایین را به شبکه ارسال کند، و بعد از ارسال متوجه این موضوع شود که تأیید آن زمان زیادی خواهد برد، در این صورت این کاربر می تواند تراکنش اولیه را با تراکنش جدیدی که کارمزد بالاتری به ماینرها پرداخت می کند، جایگزین و از این طریق زمان تأیید تراکنش مورد نظر را کوتاه تر کند.

به کارگیری از ویژگی آر بی اف فقط در شرایطی مجاز است که تراکنش مورد نظر همچنان در مempool قرار داشته باشد و به محض تأیید شدن تراکنش، جایگزین کردن آن امری ناممکن و بیهوده است. همچنین این ویژگی می بایست در زمان ساخته شدن تراکنش برای اولین بار فعال شده باشد، در غیر این صورت نمی توان آن را به کار بست. فعال سازی آر بی اف از راه تنظیم مقداری است که در یکی از متغیرهای تراکنش به نام توالی ورودی درج می شود. به این صورت که اگر عدد درج شده در زمان ساخت تراکنش از 0xffffffff کمتر باشد، از نظر قوانین شبکه این تراکنش تا زمانی که

در مم پول قرار دارد، امکان جایگزین شدن دارد.

ترفند شناسایی از روی مقادیر رُند

Round Amounts Heuristic

این ترفند که با نام شناسایی از روی باقی مانده پول نیز شناخته می شود، یکی از روش هایی است که برای تجزیه و تحلیل داده های زنجیره بلاک به کار گرفته می شود تا مشخص شود کدام خروجی از مجموعه خروجی های یک تراکنش را می توان به عنوان پرداخت به یک فرد دیگر، و کدام را به عنوان برگشت باقی مانده پول به ارسال کننده تراکنش در نظر گرفت. این ترفند مقادیر خروجی ها را به عنوان معیاری برای شناسایی آن ها قرار می دهد. اشاره به این نکته ضروری است که این ترفند نیز مانند دیگر ترفندهایی که برای شناسایی و تجزیه و تحلیل اطلاعات زنجیره بلاک به کار گرفته می شوند، قطعی نیست و خطا دارد.

به عنوان مثال اگر یک تراکنش دو خروجی با مقادیر ۰.۱ بیت کوین و ۰.۳۱۸۳۸۴۷۷ بیت کوین داشته باشد، می توان با احتمال بالایی فرض را بر این گذاشت که خروجی اول به عنوان پرداخت به فرد دیگری ارسال شده و خروجی دوم باقی مانده پول، و به ایجاد کننده تراکنش بازگردانده شده است. ترفند شناسایی از روی مقادیر رُند برای شناسایی خروجی هایی که مقادیر آنها در صورت تبدیل به یکی از پول های فیات مثل دلار آمریکا یا ریال رُند می شوند نیز قابل تعمیم است.

(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. بازبینی فنی این اثر با نظارت [@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