فرهنگ توصیفی اصطلاحات بیت‌کوین

نسخهٔ اول

وب‌سایت منابع فارسی بیت‌کوین

سخنی با خوانندگان

درک بیت‌کوین برای افرادی که به تازگی با آن آشنا شده‌اند بسیار دشوار است. به این دلیل که پیش‌نیاز درک بیت‌کوین، کسب دانش پایه‌ای در حوزه‌های متعددی است که لزوماً ارتباطی با یکدیگر ندارند. بیت‌کوین 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 مطالعهٔ زیادی نیاز دارد.

ما در سایت منابع فارسی بر این باوریم که در دسترس بودن یک فرهنگ که اصطلاحات بیت‌کوین در آن به زبانی ساده توصیف شده باشند، می‌تواند کمک بزرگی در راه یادگیری و درک بیت‌کوین به علاقه‌مندان -خصوصاً افرادی که به‌تازگی 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

تقدیم به ضیاء صدر

#

حملهٔ ۵۱ درصد

51 Percent Attack

اگر یک فرد یا نهاد متقلّب بخواهد تراکنشی را به نفع خود از یکی از بلاک‌های زنجیرهٔ بیت‌کوین حذف یا به آن اضافه کند، باید اثباتِ کار بلاکِ مورد نظر و همهٔ 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 به‌تازگی ایجاد شده‌اند، باید بلاک‌های جدید را سریع‌تر از همهٔ ماینرهای حاضر در شبکه تولید کند. زیرا نودهای شبکهٔ بیت‌کوین همواره طولانی‌ترین زنجیره‌ای که دارای بیشترین اثباتِ کار است را به‌عنوان زنجیرهٔ معتبر قبول می‌کنند.

یک ماینرِ متقلّب، برای رسیدن به این هدف باید ۵۱ درصد از قدرتِ استخراجِ شبکهٔ بیت‌کوین را در اختیار داشته باشد. به عبارت دیگر، توان محاسباتی او باید از مجموعِ توان محاسباتی سایر ماینرها بیشتر باشد. اجرای چنین حمله‌ای روی شبکهٔ بیت‌کوین تقریباً ناممکن است، بنابراین شبکهٔ بیت‌کوین در برابر کلاه‌برداری و برگشت خوردن تراکنش‌ها مصون است. برگشت‌ناپذیری تراکنش‌ها بدان معنی است که بازپس‌گیری بیت‌کوین‌های ارسال شده -پس از تأیید- به‌هیچ‌وجه ممکن نیست.

ترس از حملهٔ ۵۱ درصد باعث می‌شود که میزان توان هش موجود در شبکه اهمیت داشته باشد، زیرا نرخ توان هشِ موجود در شبکه درواقع نمایانگر کل ظرفیت استخراج شبکهٔ بیت‌کوین است و هرچه این عدد بیشتر باشد، اجرای یک حملهٔ ۵۱ درصدی گران‌تر خواهد بود. بنابراین میزان توان هشِ موجود در شبکه، معیاری برای سنجشِ امنیت شبکه در برابر حملهٔ 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 بیت‌کوین و برخی از آلت‌کوین‌ها مورد استفاده قرار می‌گیرد. وی از اولین افرادی است که روی بیت‌کوین 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 بیت‌کوین جویا شده بود. او یکی از بنیان‌گذاران شرکت بلاک‌استریم است. این شرکت در گذشته یکی از مشارکت‌کنندگان اصلی در بهبود نرم‌افزار بیت‌کوین بوده است.

آدام بک به‌عنوان مدیرعامل شرکت بلاک‌استریم این شرکت را به یکی از توسعه‌دهندگان پیشرو در شبکهٔ لایتنینگ، زنجیرهٔ جانبیِ «لیکوئید»، و دیگر پروژه‌های جالب، تبدیل کرد. مشارکت او در بیت‌کوین 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 بیت‌کوین، و آیندهٔ توسعهٔ بیت‌کوین سخنرانی‌هایی برگزار می‌کند.

امضایِ تطبیقی
Adaptor Signature

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

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

کرد. با معلوم بودن هر ۲ داده از ۳ دادهٔ 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 محرمانهٔ طرف مقابل اطلاع داشته باشد.

به عنوان مثال، آوا و بابک قصد دارند یک بیت‌کوین با یکدیگر تهاتر کنند. ابتدا، آوا یک امضای تطبیقی از تراکنش امضاء نشده‌ای که ۱ بیت‌کوین به بابک ارسال می‌کند را به او می‌دهد. این تراکنش هنوز توسط آوا امضاء نشده است، بنابراین هنوز امکان منتشر شدن روی شبکهٔ بیت‌کوین را ندارد، ولی به مقدار محرمانه‌ای که در آن وجود دارد پایبند است. در مرحلهٔ بعد، بابک تراکنشی ایجاد می‌کند که در آن ۱ بیت‌کوین به آوا ارسال می‌شود. بابک می‌تواند امضای تطبیقیِ خود را با استفاده از امضای تطبیقیِ 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 دادهٔ مخفی را در اختیار دارد، قادر است امضایِ تراکنش بابک را تولید کند و با ارسال تراکنش به شبکه، ۱ بیت‌کوین خود را مطالبه کند. بابک به محض مشاهدهٔ تراکنش امضا شده‌اش روی زنجیرهٔ بیت‌کوین، می‌تواند با استفاده از امضای تطبیقی و امضای اولیهٔ خود، دادهٔ مخفی را محاسبه کند. با استفاده از این دادهٔ مخفی او می‌تواند امضای تراکنش آوا را بدست آورد. بابک اکنون می‌تواند تراکنش آوا را امضاء و او نیز ۱ بیت‌کوین خود را با ارسال این تراکنش به شبکه مطالبه کند.

آدرس Address

آدرس برای دریافت بیت‌کوین بکار گرفته می‌شود و به‌صورت رشته‌ای از حروف و اعداد به نمایش در می‌آید. معمولاً مفهوم آدرس و کلید عمومی به جای یکدیگر بکار گرفته می‌شوند ولی آدرس درواقع هَشِ یک کلید عمومی است. در حال حاضر برای دریافت بیت‌کوین از آدرس‌ها، و نه کلیدهای عمومی استفاده می‌شود. از نظر فنی یک آدرس علاوه بر هشِ کلید عمومی، اطلاعات بیشتری را در خود ذخیره می‌کند. کاربران می‌توانند توسط یک کیف پول بیت‌کوین به هر مقدار که نیاز داشته باشند، آدرس تولید کنند. کاربران کیف پول‌ها همچنین قادرند به آدرس‌های دیگران

بیت‌کوین ارسال کنند. هنگامی که بیت‌کوین به یک آدرس ارسال می‌شود، فقط صاحب کلید خصوصی‌ای که این آدرس از آن مشتق شده، قادر به خرج کردن یا ارسال آن برای دیگران است.

پیشنهاد می‌شود برای حفظ حریم خصوصی از یک آدرس دو بار برای دریافت بیت‌کوین استفاده نشود. هروقت قصد دریافت بیت‌کوین دارید، باید از یک آدرس جدید که توسط کیف پول شما ساخته شده است استفاده کنید.

از نظر فنی، هر آدرس نمایندهٔ یک اسکریپت است و برای نشان دادن نوع اسکریپت خود کُدبندی، و یک پیشوند مشخص به آن اضافه می‌شود. آدرس‌های قدیمی از روش کُدبندی بیس-۵۸ استفاده می‌کنند و اگر هشِ یک کلید عمومی باشند، به آن‌ها آدرس‌های نوع P2PKH گفته می‌شود و با شمارهٔ «۱» شروع می‌شوند. آدرس‌های قدیمی به ندرت هشِ یک اسکریپت هستند و در این صورت با شمارهٔ «۳» شروع می‌شوند. در حال حاضر همهٔ آدرس‌های نسخهٔ صفر سگویت از روش کُدبندی بیش-۳۲ استفاده می‌کنند و با پیشوند «bc1q» شروع می‌شوند.

هنگامی که یک کاربر آدرسی را در کیف پول خود وارد می‌کند و قصد ارسال بیت‌کوین به این آدرس را دارد، کیف پول نوع آدرس را بررسی و اسکریپت موردنیاز را تولید می‌کند. این اسکریپت scriptPubKey نامیده می‌شود و به مقدار بیت‌کوینی که باید به این آدرس ارسال شود اضافه می‌شود. این دو داده، یعنی مقدار بیت‌کوینی که قصد داریم ارسال کنیم، و scriptPubKey در کنار هم، یک خروجی تراکنش را می‌سازند.

آلت‌کوین Altcoin

پس از ظهور بیت‌کوین، شبکهٔ غیرمتمرکز و سیستم پرداخت همتا-به-همتای آن الهام‌بخش پدید آمدن یک کلاس دارایی جدید شد. بازارهای کریپتوکارنسی در نتیجهٔ موفقیت بیت‌کوین پدید آمدند و این بازار در حال حاضر شامل هزاران پروژه مختلف است. به این پروژه‌ها و کوین‌ها که از سال ۲۰۱۱ و به منظور از نو اختراع کردن بیت‌کوین و اضافه کردن ویژگی‌های جدید به آن بوجود آمده‌اند، آلت‌کوین گفته می‌شود. نخستین آلت‌کوین در آوریل سال ۲۰۱۱ و با به‌خدمت گرفتن کُد

و سیستم بلاک‌چین بیت‌کوین به‌وجود آمد و Namecoin نام داشت.

هیچکدام از جایگزین‌های بیت‌کوین که از سال ۲۰۱۱ به بعد در حال معرفی شدن هستند، نتوانستند به قیمت، کاربری، و یا امنیت بیت‌کوین نزدیک شوند و به‌صورت 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 همهٔ خدمات بانک‌ها، کارفرمایان، رسانه‌های اجتماعی، و شرکت‌های تلفن منوط به ارائه اطلاعات هویتی شخصی است.

مدارهای مجتمع با کاربرد خاص (ایِ‌سیک) — Application-Specific Integrated Circuit (ASIC)

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

از آنجا که امروزه صنعت استخراج بیت‌کوین به یک صنعت بزرگ تبدیل شده، سختیِ شبکه به حدی افزایش یافته است که دیگر بکارگیری از CPU یا GPU برای استخراج بیت‌کوین 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 بیت‌کوین مشغول هستند دستاوردهای بزرگی به دنبال دارد. دلیل

انفجار توان هشِ شبکهٔ بیت‌کوین نوآوری‌های سریعی است که در طول دههٔ گذشته در صنعت ASIC رخ داده و موجب تقویت هرچه بیشتر امنیت بیت‌کوین 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 جدیدِ ارزش توسط کارل منگر در سال ۱۸۷۱ منتشر شد. دقیقاً همان سالی که ویلیام استنلی جونز، اقتصاددان انگلیسی به‌طور مستقل نظریهٔ مشابهی را منتشر کرد.

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

نظریهٔ 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 «کاربردِ حاشیه‌ایِ» ارزش، این پارادوکس را حل می‌کند. در کل آب بسیار ارزشمندتر از الماس است و هر فَرد فقط از یک مقدار مشخص از آبی که به دستش می‌رسد برای زنده‌ماندن 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 می‌شود، در تناقض است.

B

سازگاری عقب‌رو (پساسازگاری) Backwards Compatibility

اگر یک به‌روزرسانی روی یک سیستم انجام شود و نسخهٔ قبلی را بلااستفاده نکند، به آن یک ارتقاء با سازگاریِ عقب‌رو می‌گویند. سازگاریِ عقب‌رو زمانی ممکن خواهد بود که یک بروزرسانیْ قوانین معتبرِ فعلی را در نسخهٔ جدید، نامعتبر کند. اما اگر در یک به‌روزرسانیْ قوانین نامعتبر فعلی، معتبر شوند سازگاریِ 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 سازگاریِ عقب‌رو داشته باشدْ سافت فورک، در غیر این صورت هارد فورک نامیده می‌شود.

برای نمونه، لامپ‌های LED نسبت به لامپ‌های رشته‌ایِ 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 شبکهٔ بیت‌کوین یعنی سگویت در سال ۲۰۱۷ از راه سافت فورک روی شبکه اجرا شد.

کُدبندی بِیس-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 کدبندی برای جلوگیری از سردرگمی کاربران، عدد

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

یکی از گونه‌های این روش کدبندی، روش بِیس-۵۸ با قابلیت جمع‌آزمایی است که برای نمایش آدرس‌های قدیمی بیت‌کوین و کلیدهای خصوصی در قالب WIF استفاده می‌شود. بِیس-۵۸ با قابلیت جمع‌آزمایی با بِیس-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 پیشوندْ نمایانگرِ اصلِ دادهٔ 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.

کُدبندی بِیس-۶۴ Base64

روشی است که برای کُدبندی تراکنش‌هایی که به صورت ناقص امضا شده‌اند (PSBT) به‌کار گرفته می‌شود. این روش شامل ۶۴ کاراکتر الفبای انگلیسی، یعنی همهٔ 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 به‌صورت بسیار بهینه نمایش دهد، اما خوانایی پایینی دارد. بنابراین این روش اغلب برای کدبندی داده‌هایی به‌کار می‌رود که قرار نیست توسط انسان‌ها خوانده شوند و معمولاً از روش اسکن کدهای QR بین دستگاه‌ها منتقل می‌شود.

ارسال گروهی بیت‌کوین Batching

ارسال گروهیِ 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 هرکدام 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 درخواستِ برداشت ۱۰۰ نفر از مشتریان خود را با ساختن ۱۰۰ تراکنش جداگانه انجام دهد، و همچنین می‌تواند یک تراکنش با صد خروجی بسازد. گزینهٔ دوم موجب صرفه‌جویی قابل توجهی در کارمزد تراکنش می‌شود.

کُدبندی بِش-۳۲ Bech32

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

کُدبندی بِش-۳۲اِم Bech32m

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

باینری Binary

دستگاه اعداد دودویی یا باینری سیستمی است که فقط از دو عدد استفاده می‌کند: صفر و یک. کامپیوترها در دستگاه اعداد دودویی کار می‌کنند، به این معنی که آن‌ها داده‌ها را با استفاده از صفر و یک محاسبه و ذخیره می‌کنند. به عبارت دیگر ورودی‌هایی مانند حرکت ماوس، فشار دادن دکمه‌های صفحه‌کلید 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 به‌صورت ۰۱۰۰۱۰۱۱ در سیستم باینری، و 4b در سیستم هگزادسیمال نمایش داد.

بیپ-۳۹ (کلمات بازیابی) BIP39 (Mnemonic Phrases)

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

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

بیت Bit

نام اختصاریِ «رقمِ دوتایی» است و مقدار آن یا یک است یا صفر. یک بیت کوچکترین واحد داده‌های دیجیتالی است. همهٔ داده‌های کامپیوتری به‌صورت 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 سایز 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 بیت‌کوین اشاره دارد. در این صورت هر بیت، ۱۰۰ ساتوشی یا ۱ میلیونیوم ۱ بیت‌کوین است. این واحد اکنون با گذشت زمان و به دلیل استفاده نشدن تقریباً منسوخ شده است.

بیت‌کوین Bitcoin

بیت‌کوین 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. شبکهٔ بیت‌کوین یک شبکهٔ همتا-به-همتا، و مکانیسم اجماع آن بر پایهٔ اثبات کار و یک دفتر کل غیرمتمرکز به نام بلاک‌چین است. بیت‌کوین در تاریخ ۳۱ اکتبر سال ۲۰۰۸ (مطابق با دهم آبان ۱۳۸۷ خورشیدی) توسط خالق ناشناس آن یعنی ساتوشی ناکاموتو معرفی، و شبکهٔ آن نیز در تاریخ ۳ ژانویهٔ سال ۲۰۰۹ راه‌اندازی شد.

عرضهٔ بیت‌کوین به ۲۱ میلیون کوین محدود، سیاست پولی آن ثابت، و از قبل برنامه‌ریزی شده است. هر چهار سال، نرخ عرضهٔ آن به نصف کاهش پیدا می‌کند و در نهایت به صفر می‌رسد. این یکی از خصوصیات منحصربه‌فرد بیت‌کوین در مقایسه با دیگر پروژه‌های آلت‌کوین است که عرضهٔ آن‌ها به‌صورت مداوم، غیرقابل پیش‌بینی، و بی حد و حصر ادامه دارد.

بیت‌کوین تحت کنترل یک نهاد مرکزی نیست. به جای به خدمت گرفتن معماری سرویس‌دهنده-سرویس‌گیرنده و قرار دادن یک پایگاه‌دادهٔ مرکزی در مرکز شبکه و فراهم کردن داده‌های مورد نیاز به کاربران شبکه، هریک از کاربران حاضر در شبکهٔ بیت‌کوین از یک نسخه از پایگاه دادهٔ دفتر کل حسابداری بیت‌کوین بر روی دستگاه‌شان نگهداری می‌کنند. این قابلیت به کاربران این امکان را می‌دهد که موجودی‌ها و تاریخچهٔ نقل و انتقال همه بیت‌کوین‌ها را به‌طور مستقل بررسی کنند. زنجیرهٔ بلاک‌های بیت‌کوین به‌صورتی طراحی شده است که فقط می‌توان به آن بلاک‌های جدید را اضافه کرد و به‌هیچ‌وجه نمی‌توان بلاک‌های قدیمی را تغییر داد یا حذف کرد.

بیت‌کوین bitcoin

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

بیت‌کوین کُر Bitcoin Core

بیت‌کوین کُر رایج‌ترین پیاده‌سازی پروتکلِ بیت‌کوین است و سایر پیاده‌سازی‌ها برای اطلاع از روش نگهداری از قوانین اجماع و همچنین روش به‌روزرسانی، به آن مراجعه می‌کنند. اکثر کاربران برای دریافت سورسِ بیت‌کوین آن را دانلود می‌کنند. بیت‌کوین کُر نرم‌افزاری برای نودِ 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 استفادهٔ کاربرانْ غالب است. هرکس مایل به اجرای آن به‌عنوان نرم‌افزار نود شبکه باشد می‌تواند از طریق صفحه گیت‌هاب یا وب‌سایت این پروژه، به آن دسترسی پیدا کند.

بیت‌کوین 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، نسخهٔ آخر و نسخهٔ اصلی ساتوشی همچنان با یکدیگر سازگار هستند.

بیت‌کوین کُر یک نرم‌افزار منبع باز (اپن سورس) است. این بدان معناست که هرکس می‌تواند کُد آن را تکثیر و به دلخواه خود ویرایش کند. اگر یک توسعه‌دهنده قصد دارد کُد بیت‌کوین 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 زمینهٔ

بیت‌کوین فعالیت می‌کنند بخشی از هزینه‌های این افراد را از طریق کمک‌های مالی و کمک‌های بلاعوض تأمین می‌کنند.

پیاده‌سازی‌هایِ بیت‌کوین Bitcoin Implementations

یک پیاده‌سازی بیت‌کوین درواقع یک برنامهٔ نرم‌افزاری است که کامپیوتر شما را به یک نود در شبکهٔ بیت‌کوین تبدیل، و با دیگر نودهای حاضر در شبکه تعامل برقرار می‌کند. چندین پیاده‌سازی مختلف از نرم‌افزار بیت‌کوین وجود دارد که به زبان‌های برنامه‌نویسی مختلف نوشته شده‌اند. هرکس می‌تواند کُد آن را تکثیر و تغییر دهد یا عمل‌کرد آن را شبیه‌سازی کند، زیرا بیت‌کوین یک پروژهٔ منبع باز (اپن سورس) است. این امر به جای آسیب رساندن به امنیت و کارایی بیت‌کوین، موجب تقویت آن می‌شود.

هر پیاده‌سازی، طراحی و ویژگی‌های متفاوتی نسبت به دیگران ارائه می‌کند، اما در نهایت همهٔ آن‌ها می‌بایست برای حفظ یکپارچگی شبکهٔ بیت‌کوین روی قوانین اجماع پروتکل بیت‌کوین توافق کنند. به عنوان مثال، پیاده‌سازی‌های مختلف می‌توانند از انواع کیف پول‌ها، اَشکالِ متفاوت تراکنش‌ها، برآورد هزینهٔ تراکنش، یا انتخاب کوین‌ها برای ایجاد تراکنش‌ها استفاده کَنند اما همهٔ آن‌ها باید قوانین یکسانی را در مورد اعتبار بلاک‌ها، تراکنش‌ها، و امضاهای دیجیتال اعمال کنند. در حالی که امروزه پیاده‌سازی مختلفی از پروتکل بیت‌کوین وجود دارد، نرم‌افزار بیت‌کوین کُر یعنی پیاده‌سازی اصلی‌ای که توسط ساتوشی ناکاموتو در سال ۲۰۰۸ ایجاد شد، نسبت به دیگر پیاده‌سازی‌ها غالب است و توسط افراد بیشتری مورد استفاده قرار می‌گیرد. دیگر پیاده‌سازی‌ها شامل نرم‌افزارهای `Bitcoin Knots`، `bcoin`، و `btcd` است.

پیشنهاد بهبود بیت‌کوین (بیپ) Bitcoin Improvement Proposal (BIP)

پیشنهاد بهبود بیت‌کوین یک پیشنهاد رسمی برای بهبود شبکهٔ بیت‌کوین است. ارتقاء کُد و بهبود امنیت شبکهٔ بیت‌کوین از این کانال در سورس کُد بیت‌کوین وارد می‌شوند. به‌روزرسانی‌های پروتکل بیت‌کوین از قبیل سگویت، کیف پول‌های سلسله‌مراتبیِ پیش‌بینی‌پذیر، تراکنش‌هایی که به‌صورت ناقص امضاء شده‌اند، 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 بیت‌کوین قرار گرفته‌اند. با این حال همه این پیشنهادها قصد تغییر کُد یا قوانین اجماعِ بیت‌کوین را ندارند. برخی از آن‌ها، مانند استاندارد بیپ-۳۹ قواعدی را به‌منظور تهیهٔ پشتیبان از کلمات بازیابی تعیین می‌کنند و در سایر پروژه‌های مرتبط با بیت‌کوین 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 به‌صورت مستقیم و به‌عنوان پیشنهاد تغییر کُد بر روی مخزن سورس بیت کوین ارسال می‌شوند و در همان بخش مورد بحث و بررسی قرار می‌گیرند.

نودِ بیت‌کوین **Bitcoin Node**

یک عضو گسسته از شبکهٔ همتا-به-همتای بیت‌کوین است که با همتایان خود در شبکه ارتباط برقرار می‌کند و یک شبکه تشکیل می‌دهد. یک نودِ بیت‌کوین به هر کامپیوتری گفته می‌شود که یکی از پیاده‌سازی‌های بیت‌کوین را اجرا می‌کند و همه یا بخشی از زنجیرهٔ بیت‌کوین 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 همهٔ نودهای شبکه با یکدیگر سازگاری داشته باشد، می‌توان گفت که نودهای شبکه به اجماع رسیده‌اند.

به‌منظور محافظت از قوانین اجماع، جلوگیری از اجرای کُدهای مخرب، و همچنین جلوگیری از ایجاد تغییرات در ترتیب بلاک‌ها در زنجیرهٔ بیت‌کوین، تعداد نودهای شبکهٔ بیت‌کوین از اهمیت بالایی برخوردار است.

زبان اسکریپت‌نویسی بیت‌کوین **Bitcoin Script**

به زبان اسکریپت‌نویسی بیت‌کوین «اسکریپت» می‌گویند. تمام اسکریپت‌های بیت‌کوین 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 همهٔ 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 شبکهٔ 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 زنجیرهٔ 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 دیجیتالی داریم که توسط چندین کلید خصوصی مختلف تولید شده باشد.

یکی دیگر از انواع اسکریپت، اسکریپت‌های سگویتی P2WPKH و P2WSH هستند که به‌کارگیری آن‌ها موجب صرفه‌جویی در کارمزد تراکنش خواهد شد.

وایت‌پیپر بیت‌کوین **Bitcoin Whitepaper**

وایت‌پیپر یک مقاله علمی برای معرفی یک ایدهٔ 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 سایفرپانک‌ها منتشر

کرد.

بیت‌کوین کیوت **Bitcoin-Qt**

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

بلاک **Block**

یک بلاک مجموعه‌ای است از تراکنش‌های معتبری که در شبکهٔ بیت‌کوین منتشر شده‌اند. این بلاک‌ها بر اساس تسلسل زمانی به یکدیگر متصل هستند و یک زنجیره را تشکیل می‌دهند.
بلاک‌های بیت‌کوین در حال حاضر به‌طور میانگین حدود ۲,۰۰۰ تراکنش را در خود جای می‌دهند اما این تعداد ممکن است در آینده با پیشرفت‌های پروتکل بیت‌کوین افزایش یابد. با توجه به اینکه صرافی‌های بزرگ امروزه برای پرداخت‌های خود از ویژگی ارسال گروهی بیت‌کوین 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 زنجیرهٔ بیت‌کوین اضافه شود که مقدار هش آن در چهارچوب اثباتِ کار مورد پذیرش در شبکهٔ بیت‌کوین 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 زنجیرهٔ بلاک بیت‌کوین خواهد شد. این ویژگی به دلیل ماهیت توابع هش است که قطعی و تصادفی هستند. این سیستم موجب می‌شود زنجیرهٔ بلاک بیت‌کوین تغییرناپذیر شود.

به عنوان مثال، اگر تراکنشی در بلاک شماره ۴۰۰ تغییر کند، هش این بلاک تغییر خواهد کرد و در پی آن عدد اثباتِ کار بلاک شماره ۴۰۰ دیگر معتبر نخواهد بود. ولی این مسأله به اینجا ختم نمی‌شود چرا که بلاک شمارهٔ ۴۰۱ نیز نامعتبر خواهد شد، زیرا پارامتر هش بلاک قبلی در بلاک ۴۰۱ دیگر با هش بلاک شماره ۴۰۰ مطابقت ندارد. این تغییر به‌صورت آبشاری به سمت جلو حرکت می‌کند و ارتباط همهٔ بلاک‌هایی که پس از بلاک شمارهٔ ۴۰۰ آمده‌اند را از یکدیگر قطع می‌کند. این ویژگی تضمین می‌کند که پس از اضافه شدن یک بلاک به زنجیرهٔ بلاک‌های بیت‌کوین، دیگر نمی‌توان آن بلاک یا هریک از تراکنش‌های موجود در آن را تغییر داد.

بلاک اکسپلورر (کاوشگرِ بلاک) Block Explorer

بلاک اکسپلورر سرویسی است که عموم افراد را قادر می‌سازد بلاک‌ها، آدرس‌ها، و تراکنش‌های زنجیرهٔ بیت‌کوین را مرور، و از وضعیت آن‌ها مطلع شوند. زنجیرهٔ بلاک‌های بیت‌کوین در دسترس عموم افراد قرار دارد. ده‌ها هزار نود در شبکهٔ بیت‌کوین یک نسخه از زنجیرهٔ بلاک‌های بیت‌کوین را در خود ذخیره کرده‌اند و این موضوع صاحبان آن‌ها را قادر می‌سازد تا هریک از تراکنش‌ها و بلاک‌هایی که در شبکهٔ 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 به‌شدت 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 به‌صورت محلی و بر روی نود خود اجرا کنند.

برای امتحانِ یک بلاک اکسپلورر و خدماتی که ارائه می‌کند، از سایت mempool.space بازدید، و فهرست کاملِ بلاک‌های شبکهٔ 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 بیت‌کوین 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.
- هَشِ بلاک: نمایندهٔ عدد اثباتِ کار است.
- هَش بلاک قبل: قرار گرفتن این مقدار در سربرگِ بلاک غیرقابل‌تغییر بودن بلاک‌های قبلی را تضمین می‌کند.
- برچسبِ زمان: نشان می‌دهد که بلاک موردنظر در چه زمانی منتشر شده است.
- ریشهٔ مِرکِل: هشِ همهٔ تراکنش‌هایی است که در بلاک موردنظر قرار گرفته است.
- سختیِ شبکه: این مقدار به روش خاصی کُدبندی می‌شود و با نام "bits" در سربرگ 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 سایز کوچکی که دارد می‌تواند سریع‌تر از خودِ بلاک بین نودهای شبکه منتقل و پردازش شود. ماینرها برای پیدا کردن عدد اثباتِ کارْ متغیرهای مجاز در سربرگ بلاک را تغییر می‌دهند و درواقع فقط با سربرگ بلاک سر و کار دارند و آن را هش می‌کنند.

این روش بسیار بهینه است، زیرا هرچه اطلاعاتی که می‌بایست هش شود بیشتر باشد -مانند هزاران تراکنشی که در یک بلاک قرار دارد،- به زمان و منابع بیشتری برای این کار نیاز خواهد بود. اگر

ماینرها مجبور بودند همهٔ اطلاعات بلاک را برای پیدا کردن عدد اثباتِ کار هش کنند، در این صورت ممکن بود برای بالابردن بهره‌وری خود، بلاک‌های خالی تولید کنند و این مسأله منجر به پایین آمدن ظرفیت پردازش تراکنش‌ها در شبکهٔ بیت‌کوین می‌شد.

شمارهٔ بلاک در طولِ زنجیره Block Height

یک زنجیرهٔ بلاک درواقع از بهم پیوستن بلاک‌هایی تشکیل شده است که بر اساس ترتیبِ زمانی به یکدیگر متصل، و غیرقابل تغییر باشند. بلاک‌هایی که بعد از بلاک شمارهٔ صفر -که به بلاکِ پیدایش نیز معروف است- آمده‌اند، همگی به‌صورت صعودی شماره‌گذاری می‌شوند. این شماره، درواقع شمارهٔ بلاک در طول زنجیره است.

آخرین شمارهٔ بلاک درواقع چیزی نیست جز تعداد بلاک‌های زنجیرهٔ بیت‌کوین منهای عدد یک. از این عدد همچنین می‌توان برای اشاره به یک زمان مشخص بر روی زنجیرهٔ بلاک استفاده کرد. برای نمونه، رویداد نصف شدنِ پاداشِ ساختن یک بلاک هر ۲۱۰,۰۰۰ بلاک اتفاق می‌افتد. علاوه بر این می‌توان با به‌کارگیری این شماره، بر روی تراکنش‌های بیت‌کوین قفل‌های زمانی بخصوصی ایجاد کرد.

پاداش بلاک Block Reward

یک ماینر با ساخت یک بلاک معتبر اجازه پیدا می‌کند مقدار مشخصی بیت‌کوین را در قالب یارانهٔ ساخت بلاک خلق و به آدرس خود منتقل کند. همهٔ تراکنش‌هایی که در شبکهٔ بیت‌کوین منتشر می‌شوند نیز باید مقداری بیت‌کوین به‌عنوان کارمزد به ماینرها پرداخت کنند. پاداش ساخت بلاک، درواقع حاصل‌جمع این دو مقدار است. از آنجا که یارانهٔ 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 یارانهٔ بلاک اغلب بجای یکدیگر بکار گرفته می‌شوند.

پاداش بلاک در یک تراکنش ویژه به نام کوین‌بیس به ماینر آن پرداخت می‌شود. این تراکنش

ویژه اولین تراکنش در فهرست تراکنش‌های بلاک است و ورودی ندارد. ماینرها می‌بایست برای خرج کردنِ خروجی این تراکنش ۱۰۰ بلاک صبر کنند.

وزن بلاک Block Weight

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

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

زنجیرهٔ بلاک Blockchain

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

زنجیرهٔ بلاک بیت‌کوین را می‌توان به‌عنوان یک دفترکل حسابداری دیجیتال در نظر گرفت که از حساب‌های همهٔ کاربران بیت‌کوین در شبکه نگهداری می‌کند. این زنجیرهٔ بلاک به‌مانند کتابی است که بایگانی همهٔ تراکنش‌هایی که تابحال روی شبکه بیت‌کوین انجام شده را ذخیره می‌کند. بنابراین هر بلاک، به مانند صفحهٔ جدیدی است که برای به‌روزرسانی وضعیت حساب‌های کاربران شبکه، به

این کتاب اضافه می‌شود. زنجیرهٔ بلاک شبکهٔ بیت‌کوین عمومی است و هزاران نود بیت‌کوین یک نسخه از این دفتر کل حسابداری را در خود ذخیره می‌کنند، بنابراین شبکهٔ بیت‌کوین یک شبکهٔ غیرمتمرکز است.
یکی از ویژگی‌های خاص یک زنجیرهٔ بلاک این است که تغییرناپذیر است. پس از اضافه شدن یک بلاک به این زنجیره، تغییر آن بسیار دشوار است. همانطور که بلاک‌های بیشتری به این زنجیره اضافه می‌شوند، ایجاد تغییر در بلاک‌های قبلی عملاً غیرممکن می‌شود.

بی‌تی‌سی BTC

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

بایت Byte

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

تاب‌آوری در برابر خطای بیزانس Byzantine Fault Tolerance

تاب‌آوری در برابر خطای بیزانس یک ویژگی در سیستم‌های غیرمتمرکزی است که هرکس می‌تواند بدون کسب اجازه از آن‌ها استفاده کند. این سیستم‌ها قادر به شناسایی و مردود کردن

اطلاعات نادرست و ناصحیح هستند. سیستمی که در برابر خطای بیزانس تاب‌آوری دارد، درواقع توانسته مسألهٔ ژنرال‌های بیزانس را حل کرده و قادر است در مقابل حملات سیبیل ایستادگی کند.

در یک سیستم غیرمتمرکز که برای استفاده از آن نیاز به کسب مجوز نیست، 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 شبکهٔ بیت‌کوین نودها می‌بایست راهی برای تعیین اعتبار داده‌هایی که از دیگر نودها دریافت می‌کنند در اختیار داشته باشند.

شبکهٔ 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 زنجیرهٔ بلاک بیت‌کوین جلوگیری می‌کنند. قوانین پروتکل بیت‌کوین برای اعتبارسنجی تراکنش‌ها و بلاک‌ها بسیار شفاف است و هیچ‌گونه ابهامی در آن وجود ندارد.

مسألهٔ ژنرال‌های بیزانس Byzantine Generals Problem

این مسأله شرح می‌دهد که دستیابی به یک توافق مطمئن، از راه نظریهٔ بازی‌ها در یک شبکهٔ غیرمتمرکز کار بسیار دشواری است. برای حل این مشکل همهٔ اعضاء 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 جنگیِ بیزانس، شهری را محاصره کرده‌اند. شهر در محاصرهٔ آن‌ها است، اما برای تعیین زمان حمله باید یک تصمیم جمعی بگیرند. اگر همهٔ ژنرال‌ها در یک زمان حمله کنند برندهٔ جنگ خواهند بود، اما اگر زمان حملهٔ 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 مسألهٔ ژنرال‌های بیزانس را از طریق پیاده‌سازی سازوکار اثباتِ کار حل می‌کند. بلاک‌ها فقط در صورتی از نظر همهٔ اعضای شبکه معتبر هستند که اثباتِ کار آن‌ها -که در قالب یک هَش ارائه می‌شود، معتبر باشد. این موضوع نودهای غیرمتمرکز شبکه را قادر می‌سازد تا بدون نیاز به اعتماد به یکدیگر، بر روی اعتبار یک زنجیرهٔ بلاک مشخص به توافق برسند. اثباتِ کارِ یک بلاک نمایانگر این واقعیت است که برای تولید این بلاک هزینه شده است، و به خودیِ 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، اثرِ نابرابرِ 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 زمانیِ مختلفی تجربه خواهند کرد. این موضوع در قیمت‌ها اعوجاج به‌وجود 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 شدهٔ جدید به اقتصاد، قیمت کالاها و دارایی‌ها افزایش یابند، با این حال قیمت همهٔ اجناس به یکباره بالا نمی‌رود. اثرِ 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 هزینهٔ خلق پول فیات جدید که به گروه‌های خاص - معمولا بانک‌ها- داده می‌شود، تقریباً صفر است. این بانک‌ها فرصت دارند تا این پول را برای به‌دست آوردن دارایی‌هایی که هنوز به دلیل افزایش پایهٔ 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 پایهٔ پولی اثر خود را بر قیمت‌ها می‌گذارد و قیمت‌ها نیز به‌تدریج افزایش می‌یابند. مردم عادی تاثیر رشد پایهٔ 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 به‌دست 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 نتیجهٔ اثر کانتیلان در واقع مالیاتی بر قدرت خرید شهروندان است که به‌صورت غیرقانونی از سوی دولت‌ها تعیین، و به‌صورت غیرمستقیم از آن‌ها دریافت می‌شود.

پول نقد Cash

پول نقد به دارایی گفته می‌شود که به‌عنوان واحد حساب و کتاب، ابزار پرداخت، و ذخیرهٔ ارزش استفاده شود. اما مهم‌تر از همهٔ 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 هیچ‌گونه خطری برای دارندهٔ آن ایجاد نمی‌کند.

این پول، نقدترین دارایی در یک اقتصاد است چون دارندهٔ آن می‌تواند آن را به سرعت به هرچیزی که نیاز داشته باشد تبدیل کند. استفاده از پول فیات به‌عنوان ابزاری برای پرداخت، و واحد حساب و کتاب کارآمد است اما به دلیل عرضهٔ نامحدود آن از سوی دولت‌ها، ابزار خوبی برای ذخیرهٔ ارزش نیست. امروزه بیت‌کوین نیز به‌عنوان ابزاری برای پرداخت استفاده می‌شود و با توجه به کمیابی و محدودیت عرضهٔ آن -برخلاف پولِ فیات،- روش بسیار کارآمدی برای حفظ ارزش سرمایهٔ کاربران آن است.

مقاوم در برابر سانسور Censorship Resistance

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

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

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

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

پایشِ زنجیره Chain Analysis

پایشِ زنجیره، ترفندی برای تجزیه و تحلیل زنجیرهٔ بلاک بیت‌کوین و ردیابی دارایی افراد از طریق رصدِ 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. پایشِ زنجیره یک مفهوم گسترده است و نباید با شرکت Chainalysis که در این حوزه فعالیت می‌کند اشتباه گرفته شود.

باقیِ پول Change Output

سیستم حسابداری بیت‌کوین برخلاف بانک‌ها بر پایه حساب مشتریان نیست. در عوض کاربران بیت‌کوین صاحبِ بخش‌هایی از بیت‌کوین هستند که خروجیِ خرج نشده نام دارد. این خروجی‌های خرج نشده شبیه به اسکناس هستند که اگر ارزش آن‌ها بیشتر از صورت‌حساب باشد صاحب آن‌ها یعنی فردی که بیت‌کوین ارسال کرده، مبلغی به‌عنوان باقیِ 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 قلک جدید بگذارید.

یک کاربر برای ایجاد یک تراکنش بیت‌کوین، یکی از خروجی‌های خرج‌نشدهٔ 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 به‌عنوان 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 فرستندهٔ بیت‌کوین با فرد دریافت‌کننده دارد.

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

جمع‌آزما Checksum

یک جمع‌آزما رشته‌دادهٔ کوتاهی در قالب بایت است که به انتهای قطعهٔ بزرگ‌تری از یک داده اضافه، و کار بررسی اعتبار آن را آسان می‌کند. با به‌کارگیری این روش می‌توان به آسانی از اشتباهات تایپی یا دستکاری داده‌ها جلوگیری کرد. جمع‌آزماها اغلب از چند بایتِ اولِ هشِ دادهٔ مورد نظر ساخته می‌شوند.
هنگامی که داده‌ای دارای یک جمع‌آزما باشد، هرکسی می‌تواند با بررسی آن اطمینان حاصل کند که

هشِ دادهٔ مورد نظر با این جمع‌آزما مطابقت دارد و این داده از زمان ساخته شدنِ جمع‌آزما تغییر نکرده است.

برای ساختنِ یک جمع‌آزما در پروتکل بیت‌کوین تابع هشِ SHA-256 به‌صورت دو بار پشت سرِ هم مورد استفاده قرار می‌گیرد و جمع‌آزماها در ساختن آدرس‌ها و کلیدهای خصوصی در الگوی WIF کاربرد دارند زیرا این داده‌ها بین کاربران و سرویس‌ها مبادله می‌شوند و ممکن است در حین انتقال بر اثر اشتباهات تایپی مخدوش شوند.

سی‌پی‌اِف‌پی Child-Pays-for-Parent (CPFP)

سی‌پی‌اف‌پی یک ترفند در مدیریت تراکنش‌های تأییدنشدهٔ بیت‌کوین است و هدفی مشابه با آربی‌اِف را دنبال می‌کند. آربی‌اِف این امکان را برای فرستندهٔ بیت‌کوین فراهم می‌سازد تا با افزایش کارمزد، انگیزهٔ ماینرها را برای تأیید تراکنش بالا ببرد و در نتیجه سرعت تأیید تراکنش ارسالی خود را افزایش دهد، در مقابل سی‌پی‌اِف‌پی به گیرندهٔ تراکنش این اجازه را می‌دهد تا از این راه زمان موردنیاز برای تأیید تراکنش دریافت شده را کاهش دهد.

در موقعیتی که یک تراکنش با کارمزد پایین به شبکه ارسال شده باشد گیرنده می‌تواند برای تسریع در تأیید این تراکنش، تراکنش جدیدی را ایجاد کند که بیت‌کوین دریافتی را -با وجود اینکه هنوز تأیید نشده و در مم‌پول نودهای شبکه قرار دارد،- خرج می‌کند. تراکنش دوم کارمزد بالایی برای ماینرها در نظر می‌گیرد، بنابراین این انگیزهٔ اقتصادی را برای آن‌ها ایجاد می‌کند که اگر مایل به کسب این کارمزد بالا هستند، باید تراکنش قبلی را نیز در بلاک قرار دهند. در این صورت تراکنش اولِ دریافت‌کنندهٔ بیت‌کوین علیرغم کارمزد پایین، سریع‌تر تأیید خواهد شد.

گزینش کوین Coin Selection

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

به‌عنوان مثال، اگر آوا بخواهد به بابک ۱ بیت‌کوین بدهد و کیف پول او دارای خروجی‌های خرج‌نشده‌ای در مقادیر مختلف و در مجموع ۵ بیت‌کوین باشد، کیف پول او باید از میان خروجی‌های خرج‌نشدهٔ موجود یک یا تعدادی را به‌عنوان ورودی انتخاب کند. خروجی‌های خرج‌نشده‌ای که انتخاب می‌شوند به اولویت صاحب کیف پول بیت‌کوین بستگی دارند و این موضوع اساساً مقولهٔ مهمی است. برخی از کیف پول‌ها انتخاب خروجی‌های خرج‌نشده با مقادیر بالا را در اولویت قرار می‌دهند تا با این کار از انباشت خروجی‌های خرج‌نشدهٔ 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 به‌صورتی انتخاب می‌کنند که خروجیِ باقیِ 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 کوینِ خود را با توجه به نیازهای خود در بخش تنظیمات کیف پول تعیین کنند.

تراکنش کوین‌بِیس Coinbase Transaction

تراکنش کوین‌بیس اولین تراکنشِ هریک از بلاک‌های زنجیرهٔ بیت‌کوین است. ماینرها در این تراکنش به مقدار یارانهٔ ساختِ بلاک -که در حال حاضر ۶.۲۵ بیت‌کوین است،- و همچنین جمع کارمزد همهٔ تراکنش‌هایی که در بلاک مورد نظر قرار دارند، بیت‌کوین دریافت می‌کنند.

این تراکنشْ تنها تراکنش موجود در بلاک است که ورودی ندارد ولی با توجه به اینکه بیت‌کوین‌های جدید از این طریق خلق می‌شوند، معتبر است. برای مشاهدهٔ یک تراکنشِ کوین‌بِیس، اولین تراکنش یکی از بلاک‌های زنجیرهٔ بیت‌کوین را در یک کاوشگر بلاک ببینید.

کوین‌جوین CoinJoin

کوین‌جوین یک تراکنش بیت‌کوین است با ورودی و خروجی‌های خاصی که آن را از دیگر تراکنش‌های شبکهٔ بیت‌کوین متمایز می‌کند. ورودی‌های این تراکنش برخلاف اغلب تراکنش‌های بیت‌کوین متعلق به یک نفر نیست و همهٔ خروجی‌های آن یک اندازه هستند. این ویژگی باعث می‌شود که تعیین صاحبان خروجی‌های این تراکنش برای یک ناظر بیرونی بسیار دشوار باشد.
کوین‌جوین از راه بی‌اثر ساختن ترفندهایی که شرکت‌های پایشِ زنجیرهٔ بیت‌کوین به‌کار می‌بندند موجب حفظ حریم خصوصی کاربران بیت‌کوین می‌شود. یک تراکنشِ کوین‌جوین احتمال تشخیص مالکان کوین‌های ورودی را کاهش می‌دهد.

کوین‌جوین با سرویس‌های میکس از این لحاظ متفاوت است که برخلاف سرویس‌های میکس به‌صورت امانی اجرا نمی‌شود و برای کوین‌جوین نیازی به اعتماد به سرویس‌دهندهٔ آن نیست. چرا که اختیار کوین‌ها از ابتدا تا انتهای فرآیند کوین‌جوین همواره در دستان صاحبان کوین‌ها است.
می‌توانید نمونه‌ای از یک تراکنش کوین‌جوین 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 دورِ کوین‌جوینْ 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 همهٔ خروجی‌های این تراکنش با یکدیگر برابرند.

کُلد استوریج

Cold Storage

کُلداستوریج به یک روش ذخیره‌سازی اطلاعات گفته می‌شود که در آن هیچ‌گونه ارتباطی با اینترنت یا دستگاه‌های دیگر وجود نداشته باشد. یک کیف پول کُلد استوریج شکلی از ذخیره‌سازی است و اغلب توسط بیت‌کوینرها برای نگهداری از بیت‌کوین‌هایی به‌کار می‌رود که معمولاً قرار نیست در فواصل زمانی کوتاه جابه‌جا شوند.

اگر یک کیف پولْ کلیدهای خصوصی را در حالت ایزوله و منفصل از اینترنت نگهداری کند، به آن کلد استوریج می‌گویند. با این حال، می‌توان کلیدهای عمومی این کیف پولِ کلد استوریج را در یک دستگاه جداگانه که به اینترنت متصل است وارد کرد. این روش به کاربرانِ اجازه می‌دهد تا بیت‌کوین‌ها را به‌صورت مستقیم و بدون پایین آمدن امنیتْ روی کلد استوریج خود دریافت کنند.

روش نگهداری از بیت‌کوین روی کلد استوریج امن‌تر از کیف پول‌های متصل به اینترنت است، زیرا تقریباً تمام بدافزارها از طریق اینترنت به دستگاه‌ها نفوذ می‌کنند. با این حال، این روش در کنار امنیتی که با خود به همراه می‌آورد برای کاربران دشوار است. بنابراین، بهتر است از آن برای نگهداری مقادیر بالای بیت‌کوین که به‌طور روزمره مورد استفاده قرار نمی‌گیرد، استفاده شود.

ترفندِ مالک مشترک ورودی‌های یک تراکَنش

Common Input Ownership Heuristic

یکی از مهم‌ترین ترفندهایی است توسط شرکت‌های تجزیه و تحلیل زنجیرهٔ بیت‌کوین، برای تشخیص هویت مالکان کوین‌های مورد نظر به‌کارگرفته می‌شود. در حال حاضر این ترفند فرض را بر این می‌گذارد که همهٔ ورودی‌های یک تراکنش متعلق به یک نفر هستند.

این ترفند به‌هیچ‌وجه قطعی نیست، و با توسعهٔ هرچه بیشتر بیت‌کوین غیرقابل‌اطمینان‌تر می‌شود. فن‌آوری‌هایی مانند کوین‌جوین، کوین سواپ، تراکنش‌های چندامضائی، و در آینده فن‌آوری‌هایی مثل MuSig که ادغام امضاهای کوین‌های ورودی را ممکن می‌سازد، هر چه بیشتر باعث بی‌اعتبار

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 زنجیرهٔ بیت‌کوین 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 شبکهٔ بیت‌کوین، بلافاصله تصفیه نمی‌شود بلکه ابتدا از طریق نودهای شبکه دست‌به‌دست، و به مم‌پول 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 مم‌پول 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 مم‌پول 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 بیت‌کوین‌ها به یک آدرس دیگر منتقل شوند.

اجماع Consensus

اجماعْ وضعیت مطلوب در یک سیستم غیرمتمرکز مانند بیت‌کوین 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 پایهٔ اجماع بنا شده رأی‌گیری، نمایندگی، اعتبارنامه، یا متولی‌گری وجود ندارد. رسیدن به اجماعْ مشروط به توافق میان همهٔ اعضا نیست و از آنجا که همهٔ طرف‌های درگیر اغلب با یکدیگر توافق مطلق ندارند، رسیدن به اجماعْ وضعیت مطلوب است.

اجماع در دو سطح متفاوت در بیت‌کوین مطرح است؛ اول، توافق در توسعه و نگهداری از سورس بیت‌کوین، دوم بین همهٔ نودهای موجود در شبکه که به ذخیره‌سازی و اعتبارسنجی زنجیرهٔ بیت‌کوین مشغول‌اند. در سطح سورس نرم‌افزار، هرکس قادر است پیشنهادهای خود را مبنی بر اعمال تغییر یا توسعهٔ 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 توسعهٔ پروژه بیت‌کوین 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 سلایق یک گروه برگزیده بر دیگران تحمیل نمی‌شود و هیچ فرد یا گروهی قادر به تغییر بیت‌کوین برای رسیدن به منافع خود نخواهد بود.

برای رسیدن به اجماع در سطح زنجیرهٔ بیت‌کوین، می‌بایست نرم‌افزار همهٔ نودهای شبکه با یکدیگر سازگار باشند. همهٔ 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 زنجیرهٔ اصلی بیت‌کوین و تراکنش‌های معتبری که در خود دارند. اگر نودها بر روی این پارامترها اختلاف داشته باشند، شبکه دچار گسست، و زنجیرهٔ بیت‌کوین چند پاره می‌شود. برقراری صلح میان زنجیره‌های مختلف که هرکدام 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 Cryptography

رمزنگاری یک رشتهٔ مطالعاتی بسیار گسترده و متنوع است. مطالعهٔ الگوریتم‌های هَش، رمزگزاری و رمزگشایی، کلیدهای عمومی و خصوصی، همه در حوزهٔ رمزنگاری قرار می‌گیرند. هر سه این مفاهیم اساساً مبتنی بر ریاضیات و احتمالات هستند. بیت‌کوین برای خلق یک دفتر کل غیرقابل‌تغییر، 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.

بیت‌کوین با استفاده از رمزنگاری بر پایهٔ 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 بیت‌کوین اقدام کنند. اینکه عنوان می‌شود استفاده از بیت‌کوین نیاز به کسب مجوز ندارد، بدان معنی است که کاربران برای استفاده از بیت‌کوین نیاز به اخذ تأییدیه از هیچ واسطه یا شخص ثالثی ندارند و می‌توانند مستقیماً آن را به‌کار بگیرند و اساساً تمایز بیت‌کوین با سیستم‌های بانکداری سنتی همین است.

علاوه بر این هنگامی که یک کاربر به‌منظور دریافت بیت‌کوینْ کلید عمومی خود را به کاربر دیگری ارسال می‌کند، اطمینان دارد که دریافت‌کنندهٔ کلید عمومی به‌هیچ‌عنوان قادر به سرقت بیت‌کوین‌های وی نخواهد بود. این اساساً با سیستم‌های مالی سنتی متفاوت است، چون در این سیستم‌ها به‌محض اینکه فردی اطلاعات کارت اعتباری خود را به یک فروشگاه دهد یا روی دستگاه کارت‌خوان فروشگاهی 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 اضافه‌برداشت نمی‌کنند ولی دلیل اصلی آن این است که کاربران برای پس‌گرفتن حق خود به دولت یا بانک‌ها اعتماد می‌کنند. اما در بیت‌کوین با توجه به به‌کارگیری روش رمزنگاری با کلید عمومی، نیازی به اعتماد به هیچ فرد یا نهاد متمرکزی نیست.

امانی Custodial

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

به‌عنوان مثال اغلب صرافی‌ها و کارگزارانْ 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 سرویس‌دهندهٔ امانی نمی‌تواند توسط یک کاربر معمولی مورد بررسی قرار گیرد. به‌همین ترتیب، اگر یک کاربر قصد دریافت بیت‌کوین روی یک بستر امانی را داشته باشد، باید خطر سانسور، یا مصادره شدن حساب خود را در نظر بگیرد. به همین دلیل معمولاً جامعهٔ بیت‌کوین 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 به‌منظور 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 سلطهٔ شرکت‌های بزرگ بر فناوری و مالکیت معنوی هستند. ساتوشی ناکاموتو، خالق ناشناس بیت‌کوین و تقریباً تمام توسعه‌دهندگان اولیهٔ بیت‌کوین مانند هَل فینی سایفرپانک بوده‌اند.

همانطور که در بیانیهٔ 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. ارزشِ پولْ‌کالاهایی 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 کافیست مقدار بیشتری از آن‌ها خلق شود. این فرآیند معمولاً توسط دولت‌ها و به قصد تأمین هزینهٔ 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 به‌صورت 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 نقرهٔ موجود در سکهٔ نیم دلاری را از ۹۰ به ۶۰ درصد کاهش داد، درحالی‌که بر اساس قانون هر دو سکه ارزش دلاری یکسانی داشتند.

دفترِ کل حسابداریِ غیرمتمرکز

Decentralized Ledger

به آرشیو همهٔ تراکنش‌های انجام گرفته روی یک شبکه که به‌صورت غیرمتمرکز نگهداری شود، دفتر کل حسابداری غیرمتمرکز می‌گویند. این دفتر کل با همکاری بسیاری از نودهای مستقلِ حاضر در شبکه، و بر اساس مجموعهٔ قوانین پذیرفته شده میان آنان به‌روز و از آن حفاظت می‌شود.
بیت‌کوین برای سازماندهی شبکه و حفاظت از دفتر کل حسابداری خود، از زنجیرهٔ بلاک و ساز و کار اثباتِ کار استفاده می‌کند.

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

متمرکز استفاده می‌کنند. شعب بانکْ دفتر کل مرکزی را به‌صورت دوره‌ای به‌روز می‌کنند، اما این دفتر عمومی نیست و افراد عادی نیز قادر به حسابرسی آن نیستند. پروتکل بیت‌کوین این پارادایم را تغییر، و به همهٔ افراد اجازه دسترسی مستقیم به دفتر کل را می‌دهد. هرکس می‌تواند یک تراکنش بیت‌کوین را در شبکه منتشر کند، سپس ماینرها این تراکنش را به زنجیرهٔ بلاک اضافه می‌کنند و با توجه به عمومی بودن زنجیرهٔ بلاک در شبکهٔ بیت‌کوین همه می‌توانند برای بررسی موجودی و تاریخچهٔ تراکنش‌های خود به آن رجوع کنند.

همهٔ نودهای شبکه یک نسخه از دفتر کل حسابداری بیت‌کوین را در خود ذخیره می‌کنند تا امکان هیچ‌گونه تقلب در آن وجود نداشته باشد. این روش غیرمتمرکز موجب می‌شود تا این شبکه پاشنهٔ 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 بیت‌کوین عمومی و غیرمتمرکز است. شرایط در سیستم مالی و بانک‌های سنتی متفاوت است زیرا مدیران این سیستم‌ها قادرند خودسرانه اطلاعات موجود در دفتر کل حسابداری متمرکز تحت کنترل خود را تغییر دهند و کاربران این سیستم‌ها راهی برای حسابرسی و بازبینی دفتر کل متمرکز مورد استفاده را ندارند.

حملهٔ محروم‌سازی از سرویس Denial of Service (DoS) Attack

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

اگر این حمله اگر توسط گروهی از کامپیوترها و به‌صورت توزیع‌شده انجام شود، مقابله با آن اغلب دشوارتر خواهد شد زیرا نمی‌توان صرفاً با مسدود کردن یکی از حمله‌کنندگان آن را متوقف کرد.

در شبکه‌های همتا-به-همتا و عمومی مانند بیت‌کوین، مقابله با این نوع حملات یک موضوع چندوجهی است و باید با احتیاط بیشتری انجام شود زیرا در این شبکه‌ها اغلب گزینه‌های کمتری

برای قطع دسترسی بازیگران مخرب به شبکه وجود دارد.

مسیر استخراج کلید Derivation Path

داده‌ای است که کیف پول‌های سلسله‌مراتبیِ 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 سلسله‌مراتبیِ قطعی تدوین و به‌عنوان بخشی از پیشنهاد توسعه و بهبود بیت‌کوین و با شمارهٔ ۳۲ معرفی شد.

سختی شبکه Difficulty

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

سختیِ شبکه یک پارامترِ ثابت نیست و هر ۲۰۱۶ بلاک -تقریباً هر دو هفته،- به‌روز می‌شود تا آهنگِ 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 کُدبندی شده در سربرگ بلاک به نام «بیت» قابل استخراج است. این به نودهای شبکه این اجازه را می‌دهد تا درستی عدد اثباتِ کار را بررسی، و اعتبار بلاک مورد نظر را مورد بازبینی قرار دهند.

دی‌اِل‌سی Discreet Log Contract (DLC)

به الگوی خاصی از تراکنش‌های بیت‌کوین گفته می‌شود که برای اجرای یک قرارداد هوشمند سرویس‌های مرجعی مانند اوراکل‌ها را به‌کار می‌گیرند. می‌توان از طریق به‌کارگیری دی‌اِل‌سی‌ها با استفاده از زنجیرهٔ بیت‌کوین قراردادهایی را به قصد شرط‌بندی ایجاد کرد. برای ساخت یک دی‌اِل‌سی 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 هرکدام می‌توانند به‌عنوان یک اوراکل برای دی‌اِل‌سی‌ها به‌کار گرفته شوند.

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

قضیهٔ لگاریتم گسسته (دی‌اِل‌پی) Discrete Log Problem (DLP)

قضیهٔ لگاریتم گسسته این موضوع را شرح می‌دهد که در حال حاضر هیچ روش شناخته شده‌ای برای محاسبهٔ نتیجهٔ عملگر تقسیم برای نقاطی که بر روی یک منحنی بیضوی قرار دارند، وجود ندارد. محاسبهٔ نتایج عملگر ضرب که برای به‌دست 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 قضیهٔ 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 بیت‌کوین نیز بر پایهٔ قضیهٔ لگاریتم گسسته تأمین می‌شود. بیت کوین برای پیاده‌سازی رمزنگاریِ کلید عمومیْ از منحنی بیضویِ secp256k1 استفاده می‌کند. کلیدهای خصوصی اعداد تصادفیِ بزرگی هستند. برای به‌دست آوردن کلید عمومی P روی منحنی بیضوی، کلید خصوصی sk در یک عدد ثابتِ معلوم ضرب می‌شود. با توجه به قضیهٔ لگاریتم گسسته امکان محاسبهٔ 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 تولیدکنندهٔ امضای دیجیتالْ کلید خصوصی مورد نظر را در اختیار دارد.

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

بیت‌کوین به‌عنوان یک دارایی کاملاً دیجیتال از بخش‌پذیری بسیار بالایی برخوردار است. روی زنجیرهٔ بلاک بیت‌کوین می‌توان هر بیت‌کوین 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 به‌صرفه نیست. شبکهٔ لایتنینگ به‌عنوان یک لایهٔ بیرونی روی زنجیرهٔ اصلی بیت‌کوین برای مدیریت حساب کاربران خود بخش‌پذیری هر بیت‌کوین را با تقسیم کردن هر ساتوشی به ۱,۰۰۰ واحد کوچکتر بیشتر می‌کند، اما باید توجه داشت که واحد میلی ساتوشی روی زنجیرهٔ اصلی بیت‌کوین تعریف نشده است.

یک پول را دوبار خرج کردن Double Spend

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

اقلام دیجیتالی مانند فایل‌های متنی و موسیقی را می‌توان به آسانی تکثیر کرد، اما قابلیت تکثیر شدن ویژگی مطلوبی برای یک پول نیست. مسئلهٔ دوبار خرج کردن یک پول به همین موضوع اشاره می‌کند: گیرندهٔ یک پول دیجیتال از کجا اطمینان پیدا کند پولی که دریافت کرده به‌طور همزمان به فرد دیگری نیز فرستاده نشده است؟ اعضای یک شبکهٔ پولی از کجا مطمئن باشند که دیگران پول‌هایشان را عمداً دوبار خرج نمی‌کنند؟

این مسأله در شبکهٔ بیت‌کوین از طریق استفاده از یک دفتر کل حسابداری غیرمتمرکز که همهٔ کاربران به آن دسترسی دارند، حل شده است. هنگامی که یکی از کاربران این شبکه بیت‌کوین خود را به فرد دیگری ارسال می‌کند، درواقع کوینِ ارسال شده از بین رفته و در قالب یک کوین جدید در اختیار فرد دریافت‌کننده قرار می‌گیرد. حذف این کوین در دفتر کل حسابداری بیت‌کوین که در دسترس همهٔ کاربران است ثبت می‌شود تا صاحب قبلی قادر به ارسال مجدد آن به یک فرد دیگر نباشد.

داست Dust

اگر مقدار یکی از خروجی‌های خرج‌نشده (کوین) به‌قدری کوچک باشد که پرداخت کارمزد

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

حملهٔ داست Dust Attack

گاهی اوقات یک مهاجم مقدار بسیار کمی بیت‌کوین -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 به‌عنوان یک ورودی وارد کند، در این صورت خطر نشت اطلاعات مالی خصوصی او به فرد مهاجم بسیار محتمل است.

یک حملهٔ داست شبیه به اتصال یک دستگاه ردیاب به قربانی است، با این تفاوت که در این‌جا مهاجم به‌جای ردگیری مکانیِ قربانی، از اطلاعات مالی خصوصی و میزان دارایی او اطلاع پیدا می‌کند.

اگر به‌طور ناخواسته مقداری بیت‌کوین به حساب شما واریز شد، شما نباید آن را در کنار کوین‌های دیگرِ موجود در کیف پول خود به‌عنوان ورودی یک تراکنش وارد کنید. یک حملهٔ داست در صورتی موفق خواهد بود که دریافت‌کنندهٔ داست، آن را در تراکنشی که شامل کوین‌های دیگرِ او می‌شود وارد کند.

E

ای‌سی‌دی‌اِس‌اِی 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 بیت‌کوین 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 عمومیِ منتشر شده ممکن نیست. همچنین راهی برای جعل امضاء و استفاده از آن برای یک دادهٔ متفاوت وجود ندارد. با توجه به این ویژگی‌های امنیتیْ امضاء دیجیتال ECDSA در تراکنش‌های بیت‌کوین به‌کار گرفته شده است.

برای ساختن کلید عمومی، یک کاربر ابتدا باید یک کلید خصوصی تولید کند که درواقع چیزی جز یک عدد بزرگ نیست. سپس این کلید خصوصی باید در مختصات یک نقطهٔ تعریف‌شده به نام نقطهٔ مولد ضرب شود تا کلید عمومی به‌دست 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 به‌دست آورد.

حملهٔ 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. به‌عنوان مثال، اگر

یک نود بیت‌کوین با ۸ نود دیگر در ارتباط باشد و همهٔ 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 بقیهٔ شبکه همچنان به کار پردازش و دست‌به‌دست کردن بلاک‌ها مشغول است، نودِ قربانی اطلاعی از آن‌ها پیدا نخواهد کرد.

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

کُدبندی Encoding

پروتکل بیت‌کوین برای نمایش اطلاعات از روش‌های کدبندی مختلفی استفاده می‌کند. این روش‌ها بسته به نوع دادهٔ مورد نظر و به‌منظور خوانایی هرچه بیشتر و صرفه‌جویی در فضای موردنیاز روی دیسک انتخاب می‌شوند. هرچه تعداد کاراکترهای به‌کار گرفته شده در یک روش کدبندی بیشتر باشد، دادهٔ خروجی متراکم‌تر و کوتاه‌تر خواهد بود. با این حال، برخی از کاراکترها مانند عدد صفر و حرف O 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 بیت‌کوین 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 روشْ کدبندی شده‌اند اغلب با پیشوند 0x آغاز می‌شوند. کلیدهای عمومی، هَش‌ها، اسکریپت‌ها، 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 O 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 روشِ 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 دوکاراکتر + و / تشکیل شده است. تراکنش‌هایی که به‌صورت ناقص امضاء شده‌اند از این روش کدبندی می‌شوند.

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

کدهای QR: از این روش کدبندی برای نمایش اطلاعات به‌صورت تصویری استفاده می‌شود و خروجی آن عموما به‌شکل 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 درخواست‌پرداخت‌های لایتنینگ از این روش استفاده می‌شود.

رمزگذاری Encryption

به فرآیند تبدیل داده‌های آشکار و قابل فهم به فرمتی نامفهوم رمزگذاری می‌گویند. داده‌ها به‌گونه‌ای رمزگذاری می‌شوند که فقط برای افراد خاصی که صلاحیت دارند قابل خواندن باشند. فرآیند رمزگذاریْ دادهٔ 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 خواندنِ» اولیه کافیست مسیر برعکس که به فرآیند «رمزگشایی» معروف است اجرا شود.

تقریباً توسط همهٔ دستگاه‌ها و خدمات دیجیتال برای حفاظت از داده‌ها در برابر دسترسی‌های غیرمجاز و مهاجمان خراب‌کار از رمزگذاری استفاده می‌کنند. روش‌های رمزگذاریِ 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 هرکدام 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 رمزگذاریِ 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 جولیوس 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 متحدهٔ 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 دادهٔ موردنظر را با استفاده از یک کلید عمومی رمزگذاری کنند، و رمزگشایی این دادهٔ 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 عمومیِ بابک برای رمزگذاری پیام خود استفاده می‌کند و آن را برای بابک ارسال می‌کند. او نیز

هیچ‌گونه نگرانی از اینکه چه کسی به آن دسترسی پیدا می‌کند ندارد. زیرا در طول مسیر ارتباطی هیچ‌کس قادر به خواندن و درک پیام ارسال شده به بابک نخواهد بود. بابک پس از دریافت پیام رمزگذاری شده می‌تواند آن را با استفاده از کلید خصوصی خود رمزگشایی، و محتوای پیام را بخواند.

رمزگذاریِ سرتاسر End-to-End (E2E) Encryption

پیام‌های رد و بدل شده در یک شبکهٔ ارتباطی که ویژگی رمزگذاریِ سرتاسر در آن پیاده‌سازی شده باشد، تنها توسط فرستنده و گیرندهٔ پیام‌ها قابل خواندن است. رمزگذاریِ سرتاسر به کاربران این امکان را می‌دهد که بدون نیاز به اعتماد به یک شخص یا نهاد ثالث به‌صورت خصوصی با دیگران ارتباط برقرار کنند.

هنگامی که یک پیام به‌صورت سرتاسر رمزگذاری شده باشد، فرستندهٔ پیام آن را با استفاده از کلید عمومیِ گیرنده رمزگذاری می‌کند و هیچ شخص یا نهاد حتی گردانندگان بستر نرم‌افزار پیام‌رسانی که مورد استفاده قرار گرفته، قادر به رمزگشایی این پیام نخواهند بود. این قابلیت به کاربران این اجازه را می‌دهد تا برای برقراری ارتباط با یکدیگر از سرویس‌های متمرکز موجود استفاده کنند و هیچ‌گونه نگرانی بابت فاش شدن محتوای گفتگوها برای دیگران به هر دلیل ممکنی، نداشته باشند.

امروزه اغلب ارتباطات دیجیتال توسط شخص یا شرکت ثالثی که درواقع نقش تسهیل‌کنندهٔ این ارتباط را بازی می‌کند، انجام می‌شود. هنگامی که شما برای کسی ایمیل می‌فرستید، این ایمیل ابتدا به سرور یک شرکت ثالث مثل گوگل فرستاده می‌شود، سپس این شرکت ایمیل ارسال شده را به گیرنده می‌فرستد. اگر ویژگی رمزگذاریِ سرتاسر در یک ارتباط مورد استفاده قرار نگرفته باشد، افرادی که به سرورهای سرویس به خدمت گرفته شده یا شرکت‌های و نهادهای ثالث به دلایل مختلف قادرند محتوای ایمیل ارسال شده را بخوانند.

فرمان اجرایی ۶۱۰۲ Executive Order 6102

به موجب مصوبهٔ 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 این‌صورت 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 سرمایهٔ 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 شهروندانْ 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 مصادرهٔ عمومی طلای شهروندان در طول تاریخ رخ داده است. مصادرهٔ 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 به‌دلیل فیزیکی بودن بسیار دشوار است. این ویژگی منفیْ صاحبان طلا را ترغیب می‌کند تا طلای خود را نزد بانک‌ها یا دیگر مؤسسات امانی نگهداری کنند. اشکال بانک‌ها و مؤسسات امانی این است که تحت فرمان دولت‌های متبوع خود هستند. مصادرهٔ طلا از میلیون‌ها شهروندی که آن را بدون واسطه در اختیار دارند از مصادرهٔ آن از بانک‌ها و مؤسساتی که گوش به فرمان دولت هستند، بسیار بسیار دشوارتر است.

F

کارمزد تراکنش بیت‌کوین

Bitcoin Transaction Fee

یکی از مواردی که ماینرها را به فعالیت در شبکهٔ بیت‌کوین تشویق می‌کند، کسب کارمزد تراکنش‌های قرار داده شده در یک بلاک است. هرچه مقدار کارمزدی که یک تراکنش پرداخت می‌کند بیشتر باشد، ماینرها انگیزهٔ بیشتری برای تأیید آن خواهند داشت، به عبارت دیگر این تراکنش در زمان کوتاه‌تری تأیید خواهد شد. از آنجا که فضای بلاک‌های بیت‌کوین 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 بیت‌کوین مقدار کارمزد را بر اساس sats/vByte، یعنی «ساتوشی به ازای فضای مجازی اشغال شده در بلاک» نمایش می‌دهند.

کارمزد تراکنش در شبکهٔ بیت‌کوین 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 به‌کارگیری نسخه‌های جدید تراکنش‌ها، خصوصاً سگویت در کارمزد تراکنش صرفه‌جویی کرد.

فاست

Faucet

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

بیت‌کوین استفاده می‌کردند. امروزه این وب‌سایت‌ها به‌شدت نادر هستند و اگر هم وجود داشته باشند، ارقام بسیار بسیار پایینی بیت‌کوین به افراد می‌دهند.

در حال حاضر فاست‌هایی برای توزیع بیت‌کوین‌های مشقی وجود دارند. این کوین‌ها ارزشی ندارند و فقط می‌توان از آن‌ها روی شبکهٔ تست بیت‌کوین استفاده کرد.

پولِ فیات Fiat Currency

به پول‌های ملی رایج در دنیا پولِ فیات گفته می‌شود که از کلمهٔ لاتین Fiat، به‌معنی «تعیین‌شده» گرفته شده است. ارزش پول فیات توسط دولت‌هایی تعیین می‌شود که آن را خلق کرده‌اند و به‌عنوان وجه قانونی در معاملات می‌پذیرند. از آنجا که چاپ پول برای دولت‌ها هزینه‌ای ندارد، آن‌ها می‌توانند هروقت و به هر اندازه‌ای که می‌خواهند از آن پول، خلق کنند.

قدیمی‌ترین 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 همهٔ کشورها در دوره‌هایی از تاریخ در این کار موفق بوده‌اند. با این حال بیشتر پول‌ها در بلندمدت از تورم مصون نمانده‌اند و این مسأله برای کسانی که پول‌شان را پس‌انداز می‌کنند مشکل‌ساز است.

فورک (انشعاب) Fork

یک فورک زمانی اتفاق می‌افتد که بخشی از یک پروتکل یا قسمتی از کُد یک نرم‌افزار بعد از اجرای عملیات ارتقاء یا به‌روزرسانی، تغییر کند. فورک‌ها در حوزهٔ نرم‌افزار و پروژه‌های اپن‌سورس رخ می‌دهند زیرا کاربران هر زمان بخواهند می‌توانند نسبت به دانلود و اجرای نسخه‌های مختلف این

نرم‌افزارها اقدام کنند و همهٔ کاربرانِ یک نرم‌افزار لزوماً نسخهٔ آخر آن را دریافت نمی‌کنند. اگر دو کاربر نسخهٔ اول یک نرم‌افزار را دانلود و آن را اجرا کنند، و فقط یکی از آن‌ها پس از منتشر شدن نسخهٔ دومِ این نرم‌افزارْ آن را به‌روزرسانی کند، کاربری که نرم‌افزار خود را به نسخهٔ بعدی ارتقاء داده، یک فورک از نسخهٔ اول را اجرا می‌کند.

این مسأله می‌تواند برای سیستم‌هایی مانند بیت‌کوین که در آن برای تعیین دارایی افراد نیاز به اجماع است، مشکل‌ساز باشد. اگر نودهای شبکه نرم‌افزارهای متفاوتی اجرا، و در نتیجه قوانین پروتکل متفاوتی بر روی شبکه اعمال کنند، ممکن است روی معتبر بودن یا نبودن برخی از بلاک‌ها و تراکنش‌ها در شبکهٔ بیت‌کوین با یکدیگر به توافق نرسند. در این صورت شبکه دچار از هم گسیختگی و توافق روی دفتر کل غیرمتمرکز بیت‌کوین -که اصلی‌ترین حقیقت موجود در شبکهٔ بیت‌کوین است،- خدشه‌دار خواهد شد. دلیل انتخاب روش توسعهٔ محافظه‌کارانه و محتاط بودن توسعه‌دهندگان بیت‌کوین نیز همین است.

فورک‌ها 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 نسخه‌های قدیمی و جدید نمی‌شود. بنابراین لازم نیست همهٔ نودهای شبکه در این روشْ نرم‌افزار خود را به‌روزرسانی کنند زیرا قوانین نسخهٔ جدید ویژگی پساسازگاری دارند. در مقابلْ هارد فورک‌ها این ویژگی را ندارند، بنابراین برای به‌منظور ارتقاء قوانین شبکه همهٔ نودها مجبور به به‌روزرسانی نرم‌افزار خود هستند. فعالان بیت‌کوین تا حد ممکن از اجرای هارد فورک اجتناب می‌کنند و به‌شدت به سافت فورک‌ها علاقه‌مندند.

هنگامی که یک پروژه برای به‌روزرسانی قوانین پروتکل از روش هارد فورک استفاده کند و بخشی از کاربران همچنان نسخهٔ قدیمی را اجرا کنند، شبکه دچار ازهم‌گسیختگی و به دو شاخه تقسیم می‌شود. این اتفاق چندین بار در شبکهٔ بیت‌کوین رخ داده است، زیرا برخی از پروژه‌ها تلاش کرده‌اند تا از قوانین پروتکل بیت‌کوین خارج شوند و آن را برای خود تغییر دهند. به این پروژه‌ها که از قوانین پروتکل بیت‌کوین سرپیچی کرده‌اند نیز فورک گفته می‌شود، اما آن‌ها دیگر بخشی از پروژهٔ بیت‌کوین و شبکهٔ آن نیستند. این پروژه‌ها ممکن است موجب به‌وجود آمدن سردرگمی

اجتماعی شوند اما در سطح پروتکل تهدیدی برای بیت‌کوین به شمار نمی‌آیند.

فانجیبل بودن (تعویض‌پذیری) Fungibility

یک ویژگی برای کالاهایی است که می‌توان آن‌ها را با یکدیگر تعویض کرد و وقتی کنار هم قرار می‌گیرند نمی‌توان آن‌ها را از یکدیگر تمیز دارد. بهترین نمونه از یک کالای فانجیبل، سکه‌هایی است که در گذشته به‌عنوان پول خُرد مورد استفاده قرار می‌گرفت اما در حال حاضر با توجه به کاهش ارزش پول تقریباً منسوخ شده‌اند. به عنوان مثال هرکدام از سکه‌های ۵۰۰ تومانی که در گذشته رایج بودند، ۵۰۰ تومان ارزش داشتند و برای کسی که ۵۰۰ تومان از شما طلب داشت فرقی نمی‌کرد کدام‌یک از سکه‌های ۵۰۰ تومانی خود را به او بدهید.

فانجیبیلیتی یکی از ویژگی‌های مطلوب بیت‌کوین است زیرا کارآمدی آن را به‌عنوان یک ابزار پرداخت برای عموم افراد بیشتر می‌کند. به عنوان مثال اگر کوین‌هایی که در گذشته در مالکیت مجرمان بوده‌اند را بتوان از بقیهٔ کوین‌ها تمیز داد، ممکن است صرافی‌ها و فروشندگان تمایلی برای پذیرش آن‌ها نداشته باشند. در این صورت پذیرندگان بیت‌کوین باید برای اطمینان از لکه‌دار نبودن کوین‌ها، هرکدام از آن‌ها را به‌صورت جداگانه مورد بررسی قرار دهند. این محدودیت‌ها با توجه به دشواری‌هایی که برای کاربران، پذیرندگان، صرافی‌ها به‌وجود می‌آورد، عموم مردم را از پذیرش و استفاده از بیت‌کوین دلسرد و ناامید خواهد کرد.

راه‌حل‌های حفظ حریم خصوصی مانند کوین‌جوین با مخفی نمودن مالکان قبلی یک کوین از راه‌های مطمئن و امن، برای فانجیبل بودن بیت‌کوین، و بی‌معنی شدن مفهوم کوین‌هایِ لکه‌دار، تلاش می‌کنند.

G

نظریهٔ بازی Game Theory

نظریهٔ بازی مطالعهٔ ریاضیِ تضادها و استراتژی‌هایی است که برای اتخاذ مؤثرترین تصمیم بر اساس قوانین از پیش تعیین‌شده، مورد تحلیل قرار می‌گیرد. این نظریه به‌عنوان یک ساختار ارزشمند برای مفهوم‌آفرینی 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 قیاسِ نظریهٔ 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، هرکدام 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 زندانیِ 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.

مسألهٔ ژنرال‌های بیزانس

مسألهٔ ژنرال‌های بیزانس یکی از قیاس‌های معروف نظریهٔ بازی است. این مسأله با حملهٔ تعدادی از ژنرال‌ها به بیزانس آغاز می‌شود. آن‌ها شهر را محاصره کرده‌اند و باید به‌اتفاق 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 همهٔ ژنرال‌ها به‌طور همزمان به شهر حمله

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

سیستم‌های غیرمتمرکز با مسألهٔ 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 قیاسِ 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 بیت‌کوین برجسته‌ترین نقص پولِ فیات را اینگونه توضیح می‌دهد: «مشکل ریشه‌ای پول‌های رایج این است که باید به آن‌ها اعتماد کنیم تا کارایی داشته باشند.»

امروزه مسألهٔ ژنرال‌های بیزانس به طور فزاینده‌ای محبوب شده است زیرا الگوریتم اثباتِ کار بیت‌کوین اولین راه درستِ نظری برای حلِ این مشکل است. پول‌های غیرمتمرکز با مسألهٔ 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.

نقطهٔ مولّد Generator Point

نقطهٔ مولد که با نماد G شناخته می‌شود، نقطه‌ای است که روی منحنی بیضوی secp256k1 بیت‌کوین 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 Graphical User Interface (GUI)

رابط کاربری گرافیکی، یک برنامهٔ نرم‌افزاری است که به کاربران اجازه می‌دهد به صورت بصری با نرم‌افزاری که در لایهٔ پایین‌تر 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 بیت‌کوین کُر 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.

قانون گرشام Gresham's Law

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 به‌کارگرفته 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، به‌عنوان ابزاری برای ذخیرهٔ ارزش مورد استفاده قرار می‌گیرد نیز همین است.

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

قابل مشاهده است. به عنوان مثال دولت ایالات متحده آمریکا در سال ۱۹۶۵ مقدار نقرهٔ 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 به‌عنوان 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

هَوینگ
Halving

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

در ابتدای کار شبکهٔ بیت‌کوین، یارانهٔ ساخت هر بلاک ۵۰ بیت‌کوین بوده است. با این حال، رویدادی که به هوینگ 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 یارانهٔ ساخت بلاک به صفر برسد، زمانی که بیش از ۷ میلیون بلاک در ۳۴ هوینگ ساخته شده است.

سقف عرضه
Hard Cap

مجموع عرضهٔ بیت‌کوین هرگز از ۲۱ میلیون بیت‌کوین یا ۲.۱ کوادریلیون ساتوشی تجاوز نخواهد کرد. سقف عرضه یک ویژگی است که کمیابی مطلق بیت‌کوین را تضمین می‌کند و موجب می‌شود بیت‌کوین به سرنوشت بسیاری از پول‌های فیات که همانا اَبَرتورم 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.

هارد فورک

Hard Fork

به‌طور کلی فورک یعنی ایجاد یک تغییر در سورس کُد یک پروژه نرم‌افزاری. بیت‌کوین یک پروژهٔ 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.

به‌طور 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. به‌منظور حفظ اجماع پس از اعمال یک هارد فورک، همهٔ 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 به‌عنوان بلاک‌ها و تراکنش‌های معتبر می‌پذیرند. به همین دلیل است که در روند ارتقاء پروتکل بیت‌کوین 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 ذخیرهٔ کلیدهای عمومی و خصوصی و امضای تراکنش‌ها است. کیف پول‌های سخت‌افزاری به کاربران این امکان را می‌دهند تا بیت‌کوین‌های 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 سخت‌افزاریِ مختلف از نظر امنیت، حریم خصوصی، و قابلیت اطمینان با یکدیگر متفاوت

هستند.

توابعِ هَش Hash Function

تنوع توابعِ هش بسیار بالاست، اما توابع هَش به‌کار گرفته شده در حوزهٔ رمزنگاری در ویژگی‌های کلیدی زیر مشترک هستند.

- همهٔ 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 تابعِ هشِ 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 خروجیِ یک تابع هَش وجود ندارد.
- خروجیِ یک تابع هشْ 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 هش 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 هش کردن کلید عمومی یا اسکریپت، امنیت، حریم خصوصی، و راحتی را برای کاربران به ارمغان می‌آورد. هش کردن تراکنش‌ها و بلاک‌ها روشی ساده برای ایجاد شناسه‌های غیرتکراری برای آن‌ها می‌شود. در نهایت این توابع برای محاسبهٔ درخت مِرکل به‌کار گرفته می‌شوند. درخت مِرکل 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 هشْ کاربردهای مختلفی در بیت‌کوین دارند. تابع هش SHA-256 برای تولید عدد اثباتِ کار و همچنین برای تولید شناسهٔ تراکنش، دو بار پشت سر هم به‌کار گرفته می‌شود.

از تابع هش HASH160 برای تولید هشِ کلیدهای عمومی یا آدرس‌های قدیمی بیت‌کوین استفاده می‌شود. این تابع ترکیبی از دو تابع هش SHA-256 و RIPEMD160 است.

مقدارِ هَش **Hash Rate**

عددی است که نشان می‌دهد ماینرهای شبکهٔ بیت‌کوین در مجموع قادر به محاسبهٔ چند هَش بر واحد ثانیه هستند. هر یک بار هَش، تلاشی برای تولید عدد اثباتِ کار یک بلاک معتبر است و ماینرهای شبکهٔ بیت‌کوین در سراسر جهان در هر ثانیه میلیاردها بار برای به‌دست آوردن آن تلاش می‌کنند. مقدارِ هش نشان می‌دهد که چه مقدار پول، انرژی، و توان محاسباتی به پردازش تراکنش‌ها و ایمن‌سازی شبکهٔ بیت‌کوین اختصاص داده شده است.

همچنین می‌توان از روی مقدار هَش، هزینهٔ اجرای یک حملهٔ ۵۱ درصد به شبکهٔ بیت‌کوین را با تقریب خوبی تخمین زد. زیرا اجرای یک حملهٔ ۵۱ درصد مستلزم آن است که ۵۱ درصد مقدار هَش شبکه در اختیار یک ماینر خراب‌کار باشد و هرچه مقدار هش بیشتر باشد، اجرای چنین حمله‌ای نیز گران‌تر خواهد بود و احتمال اجرای این حمله کاهش خواهد یافت.

مقدار هش بیت‌کوین در دههٔ گذشته با سرعت زیادی رشد کرده است، زیرا افزایش قیمت بیت‌کوین ماینرهای بیشتری را برای پیوستن به شبکه ترغیب می‌کند. مقدار هَش تحت تأثیر عوامل مختلفی از جمله قیمت بیت‌کوین، قیمت انرژی، آب و هوا، و قوانین محلی است.

هگزادسیمال **Hexadecimal**

هگزادسیمال یک روش کُدبندی است که از یک الفبای ۱۶ کاراکتری، شامل ارقام ۰ تا ۹ و حروف A–F استفاده می‌کند. کوچک یا بزرگ بودن حروف در این طرح اهمیتی ندارد و اغلب داده‌هایی که

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

کیف پول اِچ‌دی (سلسله‌مراتبیِ قطعی) Hierarchical Deterministic (HD) Wallet

کیف پول سلسله‌مراتبیِ قطعی اصطلاحی است که برای توصیف کیف پول‌هایی به‌کار می‌رود که از یک بذر (سید) برای تولید کلیدهای عمومی و خصوصی استفاده می‌کنند. این نوع کیف پول‌ها در پیشنهاد بهبود بیت‌کوین شمارهٔ ۳۲ معرفی، و سپس به‌عنوان یک استاندارد در بیت‌کوین پیاده‌سازی شدند. اکثر کیف پول‌ها قبل از به‌کارگیری این استاندارد، برای تولید یک آدرس جدید بیت‌کوین جفت کلید جدیدی تولید می‌کردند که ارتباطی با کلیدهای تولید شدهٔ قبلی نداشت. کاربران برای پشتیبان‌گیری از این کیف پول‌ها که کلیدهایشان را از این روش که به روش «مجموعه‌ای از کلیدهای نامرتبط 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 به‌وجود می‌آورد. اما کیف پول‌های سلسله‌مراتبیِ قطعی را می‌توان به آسانی و با ذخیرهٔ یک دادهٔ ۶۴ بایتی -متشکل از یک کلید خصوصی ۳۲ بایتی، به‌علاوهٔ ۳۲ بایت دادهٔ تصادفی، معروف به بذر (سید)، پشتیبان‌گیری کرد. برای جلوگیری از اشتباهاتی که ممکن است در روند ذخیره و بازیابی دادهٔ باینریِ بذر (سید) رخ دهد، پیشنهاد بهبود بیت‌کوین شمارهٔ 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 کلمهٔ یادآوری به کاربر نمایش داده می‌شود و در اختیار داشتن این کلمات برای بازیابی کیف پول کفایت می‌کند.

اصطلاح سلسله‌مراتبی، ساختارِ درختْ مانند کلیدها را توصیف می‌کند: کلید اصلی از بذر (سید) کیف پول مشتق می‌شود و برای تولید کلیدهای فرزند به‌کار 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 به‌کار می‌گیرد و کلید مورد نظر را استخراج می‌کند. کلید اصلی که از بذر (سید) مشتق می‌شود را با حرف m نمایش می‌دهند. برای مثال، فرزند اولِ کلید اصلی دارای مسیر استخراجِ "m/0" است، و مسیر استخراج فرزند پنجمِ 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 می‌دهد که نسخهٔ پشتیبان را تنها با ذخیرهٔ بذر (سید) تهیه کنند و نیازی به پشتیبان گیری از صدها کلید نامرتبط با یکدیگر نباشد. این قابلیت همچنین کاربران را قادر می‌سازد تا آدرس‌های جدید را بدون نیاز به کلید خصوصی و از راه به‌کارگیری کلید عمومیِ والد که با نام کلید عمومی بسط یافته یا xpub نیز شناخته می‌شود، تولید کنند. این بدان معنی است که کاربر می‌تواند 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 بیت‌کوین 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 بیت‌کوین و نمایش موجودی کیف پول را دارد و با توجه به در اختیار نداشتن کلیدهای خصوصی قادر به امضاء کردن تراکنش‌ها نیست.

هودِل HODL

هودل در جامعهٔ بیت‌کوین شبیه به یک ضرب‌المثل است که از غلط املایی کلمهٔ hold گرفته شده و به بیت‌کوینرها توصیه می‌کند در مواجهه با نوسانات شدید قیمتی که بیت‌کوین اغلب تجربه می‌کند، از فروش خودداری کنند. منشاء عبارت هودل مطلبی است که یک بیت‌کوینر مست در یکی از انجمن‌های سایت bitcointalk و در خلال یکی از سقوط‌های قیمتی بیت‌کوین نوشته است.

کیف پول داغ (آنلاین) Hot Wallet

کلمهٔ داغ اشاره به آنلاین بودن دارد، بنابراین کیف پول داغ کیف پولی است که به شبکهٔ بیت‌کوین 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 بیت‌کوین به اندازهٔ 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.

اَبَر تورم Hyperinflation

به تورم بسیار بالایی که در نتیجهٔ افزایش شدید قیمت‌ها در یک دورهٔ کوتاه پدید می‌آید، اَبَرتورم گفته می‌شود. آستانهٔ اَبَرتورم در اقتصادهای مختلف متفاوت است اما اغلب در دوران بی‌ثباتیِ اقتصاد، زمانی که دولت‌ها با سرعت بالایی پایهٔ پولی را افزایش می‌دهند اتفاق می‌افتد. اقتصادها نمی‌توانند در مقابل دوره‌های پایدار و طولانیِ اَبَرتورم 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.

I

خدشه‌ناپذیری Immutability

بیت‌کوین سطح بالایی از خدشه‌ناپذیری را در دو سطح حفظ می‌کند. سطح اول، اجماع و جنبه‌های اصلی پروتکلْ به‌خصوص سیاست پولی سخت‌گیرانهٔ بیت‌کوین است که تغییر نمی‌کند.
خدشه‌ناپذیری در این سطح توسط ده‌ها هزار نود بیت‌کوین که به‌طور مستقل یک کُد مشترک را اجرا می‌کنند و بر روی مجموعه‌ای از قوانین مشترک با یکدیگر توافق دارند، اعمال می‌شود. هیچ فرد یا نهادی، نه ماینرها، و نه دولت‌ها بدون متقاعد کردن این ده‌ها هزار نود برای موافقت با تغییرات پیشنهادی، قادر به تغییر قوانین اجماع بیت‌کوین نخواهد بود. حفظ قابلیت خدشه‌ناپذیری در این سطح موجب اعتماد سرمایه‌گذاران کلان و خُرد نسبت به کمیابی و دوام بیت‌کوین می‌شود.

سطح دوم، زنجیرهٔ بلاک است که بازنویسی (یا تغییر) تاریخچهٔ نقل و انتقال بیت‌کوین را عملاً غیرممکن می‌کند. حفظ خدشه‌ناپذیری در این سطح موجب می‌شود تا فروشندگان و تجار از بیت‌کوین به عنوان یک ابزار مبادله استفاده کنند و حتی بیشتر از پول‌های فیات به آن اعتماد داشته باشند. زنجیرهٔ بلاک بیت‌کوین به گونه‌ای طراحی و پیاده‌سازی شده است که فقط می‌توان بلاک‌های جدید به آن اضافه کرد، یعنی پس از اضافه شدن یک بلاک به زنجیره، حذف یا تغییر آن عملاً غیرممکن است. این ویژگی توسط عملگرِ هَش SHA-256 اعمال، و موجب خدشه‌ناپذیریِ تاریخچهٔ بیت‌کوین می‌شود. هنگامی که یک ماینر یک بلاک را به امید یافتن یک اثباتِ کار معتبر هَش می‌کند، هَش بلاک قبل در آن گنجانده شده است. به‌لطف ویژگی‌های توابع هَش، اگَر هَش یک بلاک درنتیجهٔ اعمال تغییرات در تراکنش‌های آن تغییر کند، عدد اثباتِ کار بلاک مورد نظر و در نتیجه کل بلاک و بلاک‌های بعد از آن نامعتبر خواهند شد.

به‌عنوان مثال، اگر زنجیرهٔ بلاک دارای ۵۰۰ بلاک باشد، هشِ بلاکِ شمارهٔ ۴۰۰ شامل هَش بلاک شمارهٔ ۳۹۹ است. اگر بلاک شمارهٔ ۳۹۹ کوچک‌ترین تغییری کند در نتیجه هشِ آن نیز تغییر خواهد کرد و باعث تغییر هش بلاک بعدی یعنی بلاک شمارهٔ ۴۰۰ خواهد شد و این روند تا نامعتبر

شدن آخرین بلاک یعنی بلاک شمارهٔ ۵۰۰ در زنجیره ادامه پیدا می‌کند. تغییر یک بلاک در زنجیرهٔ بلاک بیت‌کوین، منجر به نامعتبر شدن همهٔ بلاک‌های بعد از آن خواهد شد، این یعنی ایجاد تغییر در زنجیرهٔ بلاک بیت‌کوین بدون بازنویسی بخشی از تاریخچهٔ بلاک‌های زنجیره ممکن نیست.

اگر یک مهاجمْ اکثریتِ کل توان محاسباتی شبکهٔ بیت‌کوین را در اختیار داشته باشد می‌تواند بلاک‌های زنجیرهٔ بیت‌کوین را تغییر، و تاریخچهٔ زنجیره را از طریق حملهٔ ۵۱ درصدی بازنویسی کند. برای اینکه هزینهٔ اجرای چنین حمله‌ای فراتر از توان هر نهاد یا دولتی باشد، شبکهٔ بیت‌کوین به میزان هَش بالا و غیرمتمرکزی نیاز دارد.

تورم **Inflation**

تورم، افزایش تدریجی قیمت اجناس در اقتصاد یک کشور است و باعث پایین آمدن قدرت خرید مردم می‌شود. تورم در اقتصادهای مدرن به‌عنوان یک امر پیش‌بینی‌شده درنظر گرفته می‌شود و دلیل به‌وجود آمدن آن عمدتا رشد مداوم پایهٔ پولی توسط دولت‌های محلی یا بانک‌های مرکزی است. هنگامی که تورم به سطوح بالایی برسد، به اَبَرتورم تبدیل می‌شود.

تورم به‌طور کلی بر اساس متوسط قیمت کالاهای مشخصی که در سبد خانوار قرار دارند محاسبه می‌شود، و شاخص قیمت مصرف‌کننده نام دارد. پول‌های فیات ارزش خود را به دلیل تورم در طول زمان از دست می‌دهند و ابزار مناسبی برای حفظ ارزش دارایی صاحبان خود نیستند.

دانلود زنجیرهٔ بلاک برای بار اول **Initial Block Download (IBD)**

به فرآیند دانلود زنجیرهٔ بلاکِ بیت‌کوین برای بار اول گفته می‌شود. هنگامی که یک نود (گره) جدید که به‌تازگی راه‌اندازیِ شده برای اولین بار به شبکه بیت‌کوین می‌پیوندد، ابتدا به نودهای دیگر وصل می‌شود و سپس درخواست دانلود زنجیرهٔ بلاک را به آن‌ها ارسال می‌کند. این نود جدید فرآیند دانلود و پردازش زنجیره بلاک را از اولین بلاک شروع، و تا آخرین بلاک ادامه می‌دهد و به اصطلاح با شبکه همگام می‌شود.

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 زنجیرهٔ بلاک‌ها که بر اساس اثباتِ 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 شبکهٔ 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 دانلود بلاک‌ها می‌پردازد. این کار موجب بهینه شدن فرآیند دانلود بلاک‌ها می‌شود و همچنین برخی از قابلیت‌های کاربردی را از همان ابتدا برای کاربر آن فراهم می‌کند. یک نود بیت‌کوین در کنار انجام فرآیند دانلود و ساخت زنجیرهٔ بلاک، نسبت به ایجاد مجموعهٔ خروجی‌های خرج‌نشده (UTXO) اقدام می‌کند. این مجموعه لیست جامعی از تمام کوین‌های معتبر در شبکهٔ بیت‌کوین است که هنوز خرج نشده‌اند و هریک از نودهای شبکه به محض دریافت یک بلاک جدید، این مجموعه را به‌روزرسانی می‌کنند.

توالیِ ورودی (اِن‌سیکوئنس) Input Sequence (nSequence)

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

با پیاده‌سازی پیشنهاد بهبود بیت‌کوین به شمارهٔ 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 قابلیتْ 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 همهٔ مؤسسات مالی -مانند صرافی‌ها و کارگزاری‌ها- که سرمایهٔ مشتریان خود را در اختیار دارند، لازم‌الاجرا است. قوانین احراز هویت مشتریان جزئی از قوانین مبارزه با پول‌شویی هستند و نحوهٔ اجرای آنها در حوزه‌های قضایی مختلف متفاوت است.

L

معماری لایه‌ای
Layered Architecture

ظرفیت پردازش شبکهٔ بیت‌کوین به‌طور متوسط بین ۴ تا ۷ تراکنش در هر ثانیه است و بدیهی است که این مقدار برای انجام همهٔ تراکنش‌های مالی دنیا کفایت نمی‌کند. با توجه به برگشت‌ناپذیر (نهایی) بودن تراکنش‌های ثبت شده روی زنجیرهٔ اصلی، از آن برای تصفیهٔ 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. توسعهٔ لایه‌ای موجب افزایش ظرفیت شبکه و پایین آمدن کارمزدها در پرداخت‌های خُرد می‌شود.

توسعه‌دهندگان بیت‌کوین ترجیح می‌دهند که نوآوری و افزایش ظرفیت شبکهٔ بیت‌کوین بر روی لایه‌های بیرونی انجام شود تا زنجیرهٔ اصلی بیت‌کوین -که به لایهٔ اول نیز معروف است،- از خطرات امنیتیِ احتمالی که در نتیجهٔ نوآوری‌های نرم‌افزاری پیش می‌آید، مصون باشد.

روش توسعهٔ لایه‌ای مختص به سیستم‌های دیجیتال نیست و در سیستم‌های آنالوگ نیز به‌کار گرفته می‌شود. به‌عنوان مثال قبل از منسوخ شدن استاندارد طلا در سیستم بانکداری دنیا، پول نقدِ کاغذی به‌عنوان لایهٔ بیرونی طلا که پایهٔ پول بود، به‌کار گرفته می‌شد.

برنامهٔ سَبُک
Light Client

به برنامه‌های کاربردی گفته می‌شود که با شبکهٔ بیت‌کوین تعامل دارند اما زنجیرهٔ 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 بیت‌کوین اشاره کرد.

کاربرانِ کیف پول‌های بیت‌کوین از این برنامه‌ها برای اطلاع از موجودی بیت‌کوین و دریافت اطلاعاتِ 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 ذخیرهٔ تمام زنجیرهٔ 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-of-N

m از n

این اصطلاح شرایط دقیق یک حساب چند امضایی بیت‌کوین را توصیف می‌کند که برای انتقال موجودی آن به m امضاء از میان n کلیدِ مُجازی که از قبل تعریف شده‌اند نیاز است. یک آدرس چند امضایی بیت‌کوین آدرسی است که برای خرج کردن موجودی آن به امضای چندین کلید خصوصی مستقل نیاز است. برخی از کاربران بیت‌کوین، برای دست‌یابی به قابلیت اطمینان بالاتر و حفاظت هرچه بهتر از بیت‌کوین‌های خود، دارایی خود را به جای قرار دادن در حساب‌های تک امضایی، آن‌ها در حساب‌های چندامضایی قرار می‌دهند. در این صورت دارایی آن‌ها 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 بیت‌کوین‌های خود نگهداری می‌کنند.

بیایید فرض کنیم آوا و بابک و منوچهر می‌خواهند با هم یک شرکت تأسیس کنند و قصد دارند بخشی از سرمایهٔ شرکت را در قالب بیت‌کوین و به‌صورت شراکتی در اختیار داشته باشند. برای اطمینان از اینکه هریک از شرکا به‌طور جداگانه قادر به انتقال موجودی این حساب نیست، آوا و بابک و منوچهر تصمیم می‌گیرند این دارایی را در یک حساب چند امضایی بیت‌کوین قرار دهند. همچنین توافق می‌کنند که انتقال موجودی این حساب در گرو توافق اکثریت باشد. به این معنی که موجودی این حساب مشترک می‌تواند در صورت توافق دو نفر از آن‌ها جابه‌جا شود. روش کار به این صورت است که هرکدام از آن‌ها یکی از کلیدهای عمومی شخصی خود را با دیگران به اشتراک می‌گذارد و یک آدرس بیت‌کوین از روی آن‌ها ساخته می‌شود. به این صورت که برای انتقال موجودی حساب مشترک شرکت، به ۲ امضاء از ۳ امضاء مُجازی که در هنگام ساخته شدن آدرس تعریف شده نیاز است. به بیان دیگر حساب این شرکت یک حسابِ چند امضاییِ ۲-از-۳ است.

شبکهٔ اصلی بیت‌کوین Mainnet

معرف زنجیرهٔ بلاک و شبکهٔ اصلی بیت‌کوین است که به‌عنوان بیت‌کوین واقعی شناخته می‌شود و آن را از دیگر زنجیره‌ها و شبکه‌های بیت‌کوین که اغلب در فرآیند توسعه به‌منظور آزمون و خطا به خدمت گرفته می‌شوند و فاقد ارزش مالی هستند، متمایز می‌کند. هنگامی که فردی به شبکهٔ بیت‌کوین اشاره می‌کند درواقع منظور همان شبکهٔ اصلی بیت‌کوین است که کوین‌های آن برخلاف کوین‌هایِ دیگر شبکه‌های متفرقه مثل شبکهٔ تست و شبکهٔ سیگ‌نت، ارزش پولی دارند.

هریک از این شبکه‌ها دارای زنجیرهٔ بلاک و توکن مخصوص به خود هستند و آدرس هرکدام با یک پیشوند اختصاصی شروع می‌شود. آدرس‌های شبکهٔ اصلی بیت‌کوین با یکی از پیشوندهای ۱، ۳، یا `bc1` شروع می‌شود، در حالی که آدرس‌های شبکهٔ تست با یکی از پیشوندهای ۲، `m` یا `n`، یا `tb1` شروع می‌شود. کوین اختصاصی یک شبکه نباید به یک شبکهٔ دیگر ارسال شود. برای مثال اگر کوین شبکهٔ اصلی بیت‌کوین به یک آدرس شبکهٔ تست بیت‌کوین ارسال شود، بیت‌کوین‌های باارزش شبکهٔ اصلی می‌سوزد و از بین می‌رود و راهی برای بازیابی آن نخواهد بود. عکس این موضوع نیز صادق است.

تغییرپذیری Malleability

تغییرپذیریِ تراکنش یعنی امکان اختصاص چندین شناسهٔ معتبر به یک تراکنش بیت‌کوین و زمانی اتفاق می‌افتد که اعمال تغییر در بخشی از یک تراکنش امضاء شدهٔ بیت‌کوین موجب تغییر شناسهٔ آن شود، اما تراکنش مورد نظر همچنان معتبر بماند. از آنجا که شناسهٔ تراکنش درواقع از هَش تراکنش به‌دست می‌آید، اعمال هرگونه تغییر در دادهٔ یک تراکنش موجب تغییر شناسهٔ آن خواهد شد. این در حالی است که تغییراتی که شناسهٔ تراکنش را تغییر می‌دهند و موجب بی‌اعتبار شدن آن می‌شوند، مایهٔ نگرانی نیستند.

تغییرپذیریِ تراکنش موجب می‌شود تا توسعه‌دهندگان و کاربران قادر نباشند در یک تراکنش جدید به تراکنشی قدیمی که هنوز روی زنجیرهٔ بلاک تأیید نشده است، ارجاع دهند. این مشکل به این دلیل به‌وجود می‌آید که برای خرج کردن یک خروجی خرج نشده و در زمان وارد کردن آن به

یک تراکنش جدید، می‌بایست به شناسهٔ تراکنشی که این خروجی مورد نظر در آن قرار گرفته ارجاع داده شود. بنابراین اگر امکان تغییر شناسهٔ تراکنش وجود داشته باشد، امکان ارجاع به شناسهٔ قبلی وجود ندارد، زیرا ممکن است در زمان تأیید و ثبت بر روی زنجیرهٔ 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 دادهٔ خودِ امضاء که در همان بخش قرار دارد را تغییر دهیم.

مشکل تغییرپذیریِ تراکنش‌های بیت‌کوین از طریق اجرای سافت فورک سگویت و ارتقاء قوانین پروتکل بیت‌کوین برطرف، و اجرای نوآوری‌های بیشتری چون شبکهٔ لایتنینگ و ارتقاء تپ‌روت بر روی شبکهٔ بیت‌کوین ممکن شد. سگویتْ دادهٔ امضاء را که بخشِ تغییرپذیرِ تراکنش است از بدنهٔ اصلی جدا و به بخش مجزای دیگری به نام شاهد منتقل، و با این کار مشکل تغییرپذیریِ تراکنش‌های بیت‌کوین را به‌کلی برطرف کرد.

واسطِ معامله — Medium of Exchange

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 به‌عنوان واسطِ معامله مورد استفاده قرار گرفته‌اند اما آن‌ها همهٔ 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. بیت‌کوین در سال ۲۰۲۱ و بر اساس قانونی که به «قانون بیت‌کوین» مشهور است در کشور السالوادور و در کنار دلار آمریکا به‌عنوان 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.

مِم‌پول 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 دادهٔ کوچکی به نام مِم‌پول نگه‌داری می‌کند. این تراکنش‌ها پس از تأیید و وارد شدن به زنجیرهٔ بلاک، از مم‌پول حذف می‌شوند. نودهای شبکه تراکنش‌های مم‌پول خود را از طریق شبکهٔ همتا-به-همتای بیت‌کوین 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 شبکهٔ بیت‌کوین دارد، سایز این پایگاه داده در حالت پیش‌فرض روی ۳۰۰ مگابایت تنظیم شده اما هرشخص قادر است این مقدار را برای نود خود تغییر دهد، بنابراین مم‌پول در نودهای مختلف شبکه ممکن است حاوی تراکنش‌های مختلفی باشند.

سافت فورکِ فعال‌سازی شده توسط ماینرها (اِم‌اِی‌اِس‌اِف) Miner-Activated Soft Fork (MASF)

سافت فورک به اعمال تغییراتی در قوانین پروتکل گفته می‌شود که در صورت حمایت ماینرها، ایجاد ویژگیِ پساسازگاری در آن‌ها ممکن می‌شود و نیازی به به‌روزرسانی همهٔ 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 فورکِ 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 درصدِ میزان هش)، از اعمال قوانین جدید پشتیبانی کرده باشند.

ماینرها یکی از اعضای مهم شبکهٔ بیت‌کوین هستند زیرا تراکنش‌ها را پردازش می‌کنند و بلاک‌ها را می‌سازند، اما قوانین شبکهٔ بیت‌کوین توسط آن‌ها تعیین نمی‌شود. اگر ماینرها 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 همهٔ 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 زنجیرهٔ بلاک استخراج گفته می‌شود. ابتدا ماینرها 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 مرحلهٔ بعد ماینرها سعی می‌کنند تا عدد معتبرِ اثباتِ کار را برای این بلاک جدید پیدا کنند. این جستجو درواقع بر پایهٔ حدس و گمان است و انرژی بسیار زیادی صرف می‌کند.

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

ماینرها برای ساخت یک بلاک معتبر هیچ راهی بهتر از حدس زدن عدد اثباتِ کار و بررسی اعتبار آن ندارند، بنابراین سعی می‌کنند تا در کمترین زمان و با صرف کمترین انرژی ممکن، حدس‌های بیشتری بزنند. به تعداد همهٔ 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 همهٔ ماینرهای مشغول در شبکهٔ بیت‌کوین معیار مهمی برای تعیین امنیت این شبکه است، زیرا نشان می‌دهد که یک مهاجم برای اجرای حملهٔ ۵۱ درصدی به چه میزان هَش نیاز دارد.

استخرِ استخراج Mining Pool

صنعت استخراج به دلایل متعددی چون هزینه‌های انرژی، جذب سرمایه‌گذاری، و پیچیدگی‌های فنی، در مقیاس بزرگ بهینه‌تر است. استخرهای استخراج به ماینرهای خُرد 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 استخرِ استخراجْ بلاک معتبری را پیدا می‌کند، پاداش کسب شده میان دیگر اعضای استخر و بر اساس میزانِ هشِ 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 تامبْلر 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 بیت‌کوین‌های 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 بیت‌کوین مورد استفاده قرار می‌گیرد. این فهرست درواقع نمایندهٔ داده‌ای است که می‌توان با در اختیار داشتن آن کلیدهای یک کیف پول سلسله‌مراتبیِ قطعی را تولید کرد.

کلمات بازیابی بر اساس بیپ-۳۹ در پروتکل بیت‌کوین به‌عنوان استاندارد تعریف شده و اکثر کیف پول‌های بیت‌کوین از آن پشتیبانی می‌کنند. اکثر کیف پول‌ها همچنین به کاربران اجازه می‌دهند تا به‌منظور 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 کلمهٔ آخر نیز برای افزایش قابلیت اطمینان این روش بازیابی کلید خصوصی، به‌عنوان یک جمع‌آزما عمل می‌کند. با توجه به امکان انتخاب کلمات بازیابی از میان یک لیست ۲۰۴۸ کلمه‌ای، احتمال حدس زدن فهرست کلمات بازیابی ۲۴تایی دیگران، ۱ در $۲۰۴۸^{۲۴}$ یا $۲,۹۶ \times ۱۰^{۷۹}$ است.

چند امضایی Multisig

اغلب تراکنش‌های بیت‌کوین، 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 بیت‌کوین به آدرسی که برای خرج کردن آن به چندین امضاء که توسط کلیدهای خصوصی جداگانه‌ای تولید شده‌اند نیز وجود دارد. به این ترتیب موجودی بیت‌کوین این آدرس می‌تواند به‌طور مشترک توسط یک خانواده، شرکای تجاری، هیئت‌مدیرهٔ یک شرکت، یا هر گروه دیگری کنترل شود.

یک حساب چند امضایی اغلب به‌صورت 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. به‌عنوان 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 بیت‌کوین 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.

میوسیگ 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 بیت‌کوین از یک حساب تک امضایی تپ‌روت ندارد، زیرا می‌توان با استفاده از میوسیگ کلیدهای عمومیِ افراد ذینفع در یک حساب چند امضایی را با یکدیگر ترکیب، و یک کلید عمومی تولید کرد که نمایندهٔ همهٔ 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 میوسیگْ 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 زنجیرهٔ بلاک بیت‌کوین برای همیشه ثبت می‌شود. این مسأله گذشته از پیامدهای ناخواسته‌ای که روی حریم خصوصی کاربران دارد، موجب اِشغال فضای بلاک نیز می‌شود.

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

فرهنگ توصیفی اصطلاحات بیت‌کوین توسط مترجمین ناشناس و به سرپرستی الف.آزاد در حال گردآوری، و به‌صورت یک پروژه بلندمدت تعریف شده است. بازبینی فنی این اثر با نظارت @mytechmix انجام می‌پذیرد.

لغت‌نامهٔ شرکت ریور فایننشیال به‌عنوان مرجع نسخهٔ اول این فرهنگ مورد استفاده قرار گرفته است.

وب‌سایت منابع فارسی بیت‌کوین
پاییز ۱۴۰۰