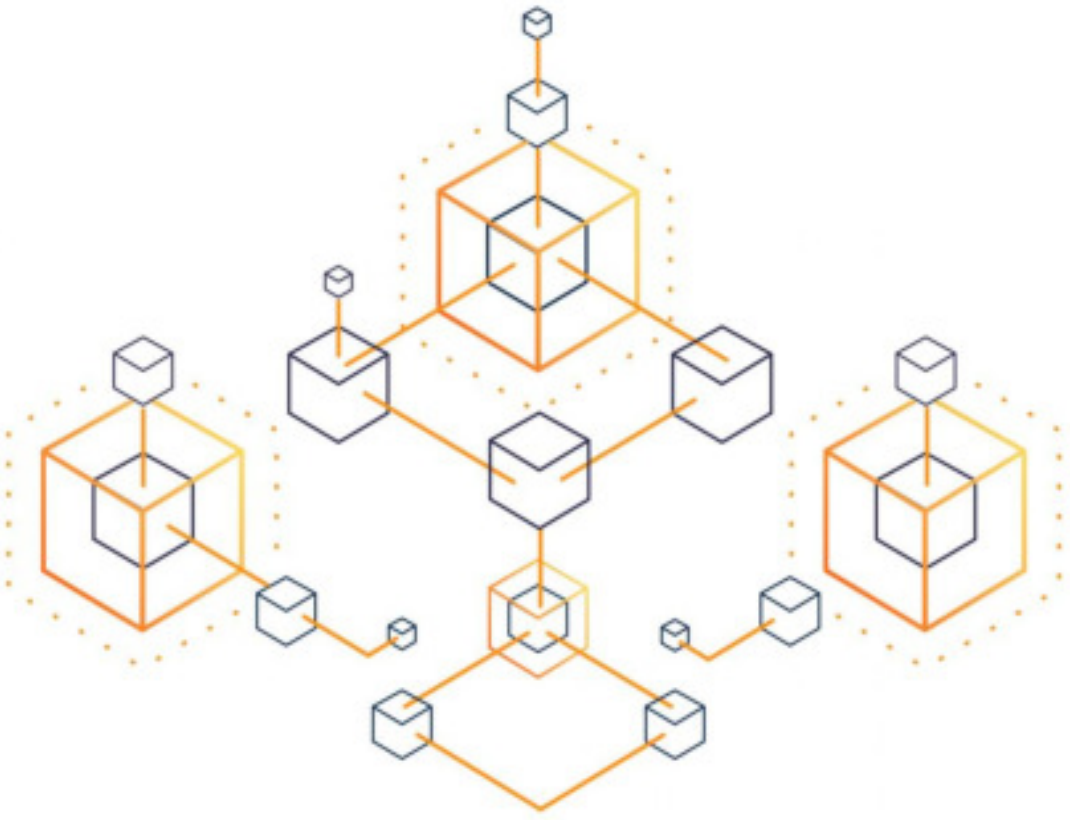
کوین ایران
CoinIran

اختراع

بیت کوین



سخنی با خوانندگان

این کتاب نحوه کار شبکه بیت‌کوین را به زبانی ساده توضیح می‌دهد. ممکن است شما به‌عنوان فردی که بخشی از دارایی خود را در بیت‌کوین سرمایه‌گذاری کرده معتقد باشید نیازی به درک نحوه کار شبکه بیت‌کوین ندارید. در این مقدمه کوتاه استدلال می‌کنیم که چرا هر فرد، در هر سطحی از توانایی فنی باید این کتاب را بخواند و به‌طور کلی از ساز و کار شبکه بیت‌کوین مطلع باشد.

اگر به تازگی با موضوع بیت‌کوین و کمیابی دیجیتال[1] آشنا شده باشید ممکن است از خود بپرسید «کنترل بیت‌کوین در دست کیست؟» برای پاسخ به این سؤال توجه شما را به قسمتی از «کتاب کوچک بیت‌کوین[2]» که ترجمه آن در همین سایت قابل دریافت است جلب می‌کنیم...

کنترل بیت‌کوین دست هیچ قدرت متمرکزی نیست. بیت‌کوین مدیرعامل یا هیئت مدیره یا شرکتی که بر آن نظارت داشته باشد ندارد. هزاران تأیید کننده تراکنش‌های شبکه بیت‌کوین در سراسر دنیا وجود دارند که بلاک‌چین بیت‌کوین را مورد بازبینی قرار می‌دهند و تاریخچه همه تراکنش‌های بیت‌کوین را در خود ذخیره می‌کنند. اسم این تأیید کننده‌ها فول نود[3] است. (نرم‌افزار بیت‌کوین که هرکس می‌تواند با اجرای آن اعتبار تراکنش‌های بیت‌کوین را بازبینی، و از درستی آن اطمینان حاصل کند)

1 Digital Scarcity
2 The Little Bitcoin Book
3 Full Node

ماینرها[4] (فرد یا گروهی که از دستگاه‌های مخصوصی برای ساختن بلاک‌های جدید در شبکه بیت‌کوین استفاده می‌کنند) در سرتاسر دنیا برای ساختن بلاک‌های بیت‌کوین با هم رقابت می‌کنند. این بلاک‌ها توسط فول نودهایی که کاربران اجرا می‌کنند بازبینی و تأیید می‌شوند. نرم‌افزاری را که این فول نودها اجرا می‌کنند «برنامه‌نویسان بیت‌کوین[5]» نوشته‌اند. تراکنش‌هایی که داخل بلاک‌های بیت‌کوین قرار می‌گیرند را کاربران بیت‌کوین با استفاده از نرم‌افزارهای کیف‌پولشان ساخته‌اند.

"همه این اجزا برای کارکرد بیت‌کوین ضروری هستند ولی هیچکدام از آن‌ها بیت‌کوین را کنترل نمی‌کنند."

اگر یک برنامه‌نویس تصمیم بگیرد یک نرم‌افزار فول نود خیلی متفاوت بسازد، ممکن است فقط تعداد انگشت‌شماری از کاربران آن را اجرا کنند و در نهایت اثری بر روی قوانین شبکه نخواهد داشت. اگر یک ماینر تصمیم بگیرد پنهانی بلاکی که اعتبار لازم را ندارد بسازد، فول نودهای کاربران آن را قبول نخواهند کرد. اگر ماینرها تصمیم به کودتا بگیرند تا کاربران را مجبور به پذیرش قابلیت‌های جدید بر روی شبکه کنند، شکست خواهند خورد چون هیچکس قادر نیست کاربران را مجبور به استفاده از نرم‌افزاری کند که نمی‌خواهند. رویداد UASF[6] نمونه تاریخی این سناریو است.

بنابراین هر تغییری در بیت‌کوین نیاز به توافق همگانی بین کاربران آن دارد. از این نظر مدل حکمرانی در بیت‌کوین شبیه به توازن قوا در حکومت‌های برپایه دموکراسی است. ماینرها شبیه به قوه مجریه به کارهای اجرایی رسیدگی می‌کنند و مجری قانون هستند، برنامه‌نویسان شبیه به قوه مقننه قوانین جدید را می‌نویسند و تصویب می‌کنند، کاربران همانند قوه قضاییه کارشان اطمینان از این است که دو قوه دیگر خارج از چهارچوب قانون اساسی کاری انجام ندهند.

4 Miner
5 Core Developers
6 User Activated Soft Fork

پس اجازه تغییر قوانین شبکه بیت‌کوین تنها در دست کاربران آن است و این وظیفه‌ای است بسیار مهم بر دوش همه بیت‌کوینرهای سرتاسر دنیا فارغ از نژاد، منطقه جغرافیایی، زبان، و مسائل سیاسی. و ما معتقدیم آگاهی از نحوه کار شبکه بیت‌کوین هرچند بسیار کلی، پیش‌نیاز انجام این وظیفه خطیر است و در مواقع بحرانی به کاربران کمک می‌کند تا تصمیم درستی بگیرند.

در پایان از nodrunner مترجم این کتاب بابت تلاش ایشان برای آگاهی‌بخشی عمومی و انتشار این کتاب به‌صورت رایگان، همچنین رسانه خبری آموزشی کوین‌ایران بابت بازبینی و صفحه‌بندی این کتاب، تشکر و قدردانی می‌کنیم.

bitcoind.me
منابع فارسی بیت‌کوین
زمستان ۱۳۹۹

بیت کوین، پول مردمی از طرف مردم برای مردم

کوین ایران مفتخر است پس از همکاری با اعضای فعال جامعه فعال بیت کوین و رمزارز ایران و ارائه کتاب **روند صعودی بیت کوین** (The Bullish Case of Bitcoin) در سال گذشته، این بار نیز در همکاری با یکی اعضای فعال جامعه بیت کوین ایران کتابی دیگر را برای مخاطبین ارجمند خود ارائه نماید.

کتاب حاضر تحت عنوان **اختراع بیت کوین** (Inventing Bitcoin) است که نسخه اصلی آن در سال 2019 منتشر گردیده است. نویسنده این کتاب آقای یان پریتزکر (Yan Pritzker) است. او در 20 سال گذشته یک توسعه دهنده نرم افزار و کار آفرین بوده است. همچنین از سال 2018 به عنوان مدیر تکنولوژی سایت Reverb.com وظیفه مدیریت تکنولوژی و زیرساخت ها را بر عهده داشته است.

به عقیده نویسنده این کتاب در پی آن است که درک درستی از فلسفه وجودی بیت کوین و بلاکچین و نحوه کار آن را برای افراد تازه کار و مبتدی توضیح دهد. به همین منظور در این کتاب به مباحث عمیق فنی پروتکل ورود نمی‌کند زیرا نویسنده بر این باور ست که در این زمینه کتاب های مفصلی مانند مسترینگ بیت کوین توسط آندریا آنتونوپولوس نوشته شده است.

این کتاب می‌کوشد که به زبان ساده ذهن مخاطبان را با علوم کامپیوتر و تئوری بازی اقتصادی بیت کوین به عنوان جذاب ترین اختراع زمانه درگیر نماید. بنابراین مطالعه این کتاب به افرادی که تاکنون هیچ آشنایی با بیت کوین ندارند و یا کسانی که آشنایی ابتدایی دارند، توصیه می‌شود.

مترجم این کتاب که هویت وی با شناسه کاربری nodrunner در توییتر شناخته می شود با کلید 6137 661C 6B65 933B نسخه اولیه ترجمه این کتاب را در اختیار کوین‌ایران قرار داده است تا با کمک تیم تحریریه کوین ایران ویراستاری و آماده انتشار شود. این مترجم ناشناس هدف خود از این کار را ترویج فرهنگ آموزش و استفاده آزاد اطلاعات برای همگان بیان می‌کند. برای نیل به این هدف، این کتاب در کتابخانه وبسایت Coiniran.com و bitcoind.me قرار داده شده است.

تیم کوین ایران امیدوار است که با ارائه این کتاب گام دیگری در جهت آگاه سازی و آشنایی جامعه مخاطب فارسی زبان برداشته و به آنها یاری رساند.

همچنین مخاطبان گرامی می‌توانند مطالب نویسنده درباره بیت کوین و موضوعات مرتبط را در سایت yanpritzker.com و در توییتر (@skwp) دنبال نمایند.

تقدیم به پدر و مادرم یوری و لانا، که خانواده ما را از اتحادیه جماهیر شوروی سابق که یک رژیم سوسیالیستی استبدادی با کنترل شدید اقتصادی بود خارج کردند.
همچنین تقدیم به همسرم جسیکا که صحبت‌های پیوسته من درباره بیت کوین و بیدار ماندن من تا پاسی از شب را برای تمام شدن این کتاب تحمل کرد.

مقدمه

به کتاب اختراع بیت کوین خوش آمدید. هدف من در این کتاب تحلیل اقتصادی بیت کوین نیست، همچنین قصد ندارم شما را متقاعد کنم که بیت کوین طلای دیجیتال است. برای این منظور کتاب bitcoin standard نوشته Saifedean Ammous را معرفی می‌کنم.

قرار نیست از زاویه سرمایه‌گذاری به بیت کوین نگاه کنم و یا دلیل بیاورم که هر فرد باید حداقل کمی بیت کوین داشته باشد. قصدِ بررسی چارت‌ها و تاریخچه قیمت بیت کوین را هم ندارم. اگر به دنبال این موضوعات هستید کتاب cryptoassets نوشته Chris Burniske و Jack Tatar را پیشنهاد می‌کنم.

همینطور ما به دنبال کاوش در نحوه عملکرد پروتکل در لایه‌های عمیق بیت کوین نیستیم، قصد بررسی کدهای کامپیوتری را هم نداریم. کتاب Mastering Bitcoin نوشته Andreas Antonopulos برای این منظور مناسب‌تر است.

به زبان ساده هدف من درگیر کردن ذهن شماست، و آشنا کردن شما با علوم کامپیوتر و تئوری بازی اقتصادی‌ای که بیت کوین را به یکی از جذاب‌ترین و قابل توجه‌ترین اختراعات زمانه تبدیل کرده است.

بیشتر افراد، اولین باری که از بیت کوین می‌شنوند چیزی از آن نمی‌فهمند. آیا بیت کوین پول جادویی اینترنتی است؟ از کجا آمده؟ کنترل‌کننده آن کیست؟ چرا به این اندازه مهم است؟

برای من تمام چیزهایی که کنار هم جمع شده‌اند تا بیت کوین را بسازند (فیزیک، ریاضیات، رمزنگاری، تئوری بازی، اقتصاد و علوم کامپیوتر) اهمیت زیادی داشت. تلاش می‌کنم در این کتاب دانش خود را به زبان بسیار ساده و قابل درک به شما انتقال دهم.

برای انتقال بهتر مفاهیم، قدم به قدم پیش می‌رویم و تنها پیش‌نیاز شما دانش ریاضیات دبیرستان است. امیدوارم این کتاب انگیزه لازم برای ورود به دنیای بیت کوین را در شما ایجاد کند.

فصل اول: بیت کوین چیست؟

بیت کوین یک پول الکترونیکی نظیر به نظیر است؛ یک پول دیجیتال که می‌تواند بین افراد و کامپیوترها بدون واسطه (مثلا بدون بانک واسط) جابه‌جا شود و ایجاد و انتشار آن تحت کنترل هیچ فرد خاصی نیست.

یک پول کاغذی و یا یک سکه فلزی را درنظر بگیرید. وقتی این پول را به کسی می‌دهید طرف مقابل نیازی نیست شما را بشناسد. کافی است مطمئن شود پولی که از شما گرفته جعلی نیست، که برای پول‌های فیزیکی معمولا با نگاه کردن و لمس پول این اطمینان حاصل می‌شود.

در حال حاضر بیشتر پرداخت‌های ما به صورت دیجیتال از طریق اینترنت و با استفاده از سرویس‌های یک واسطه انجام می‌شود. این واسطه می‌تواند یک موسسه کارت اعتباری مثل visa یا سرویس‌های پرداخت دیجیتال مانند Paypal یا Applepay و یا پلتفرم‌های آنلاینی مثل WeChat باشد.

پرداخت دیجیتال، نیازمند اعتماد به یک کنترل‌کننده مرکزی است که هر پرداخت را تایید و تصویب کند، چون پولی را که فرد می‌توانست با لمس کردن و دیدن، از جعلی نبودن آن اطمینان حاصل کند حالا تغییر ماهیت داده و تبدیل به داده‌های دیجیتالی شده است که باید توسط کسی که نقل و انتقالات را کنترل می‌کند تایید شود.

بیت کوین یک جایگزین برای کنترل‌کننده مرکزی پول دیجیتال پیشنهاد می‌کند، یک سیستم که سه جزء اساسی دارد:

1. یک دارایی دیجیتال (معمولا bitcoin که با b کوچک نوشته می‌شود)، که به تعداد محدودی وجود دارد و از قبل مشخص شده و قابل تغییر نیست. این مسئله کاملا برخلاف پولی است که ما امروزه استفاده

می‌کنیم؛ چراکه پول‌ها توسط دولت‌ها و بانک‌های مرکزی عرضه می‌شوند و نرخ انتشار آنها درطول زمان غیرقابل پیش‌بینی است.

2. یک گروه از کامپیوترهای متصل به یکدیگر (شبکه Bitcoin با B بزرگ)، که هرکسی می‌تواند به این شبکه متصل شود. این شبکه برای ردیابی مالکیت بیت کوین و انتقال آن بین اعضای شبکه به کار گرفته می‌شود و هرگونه واسطه‌ای اعم از بانک‌ها، موسسه‌های اعتباری و سرویس‌های پرداخت را حذف می‌کند.
3. نرم‌افزار کاربران بیت کوین؛ قطعه کدی که هرکسی می‌تواند آن را در کامپیوتر اجرا کند تا عضوی از شبکه باشد. این نرم‌افزار متن باز است، به این معنا که همه می‌توانند به کد آن دسترسی داشته و نحوه کار آن را ببینند و به رفع اشکالات و افزودن قابلیت‌های جدید کمک کنند.

تصویر 1: شبکه Bitcoin و پول دیجیتال bitcoin

بیت کوین از کجا آمده است؟

بیت کوین درسال 2008 توسط شخص یا گروهی اختراع شده است که با نام مستعار Satoshi Nakamato شناخته شده‌اند. هیچ‌کس از هویت واقعی این شخص یا گروه اطلاعی ندارد. در 11 فوریه 2009 ساتوشی نمونه اولیه بیت کوین را در یک فروم آنلاین متعلق به سایفرپانک‌ها عرضه کرد؛ گروهی که روی فناوری رمزنگاری کار می‌کنند و دغدغه آنها دفاع از حریم خصوصی افراد است.

تکه‌هایی از نوشته ساتوشی در زیر آمده است که در فصل بعد درباره این جملات و انگیزه‌های ساتوشی برای اختراع بیت کوین توضیح خواهم داد.

من یک سیستم پول الکترونیک به نام بیت کوین ایجاد کرده‌ام که متن باز و نظیربه‌نظیر است. کاملا غیرمتمرکز است، بدون هیچ کنترل کننده مرکزی و یا واسطه قابل اعتماد؛ چراکه به جای اعتماد همه چیز بر اساس اثبات رمز نگاری است.

مشکل ریشه‌ای پولی که در حال حاضر استفاده می‌کنیم، بحث اعتمادی‌ست که برای عملکرد آن لازم است. باید به بانک مرکزی اعتماد کرد که ارزش پول را حفظ کند. اما تاریخ پول فیات پر از نقض این اعتماد است. برای نگهداری و انتقال الکترونیکی پولهای‌مان باید به بانک اعتماد کنیم، اما بانک‌ها آن را به شکل اعتبار قرض می‌دهند. ما باید درمورد حریم خصوصی خود به آنها اعتماد کنیم. به آنها اعتماد کنیم چون اجازه نمی‌دهند سارقان حساب ما را خالی کنند. هزینه‌های کلان آنها پرداخت‌های خرد را غیرممکن می‌کند.

یک نسل قبل، سیستم‌های کامپیوتریِ چندکاربره و اشتراک زمانی هم چنین مشکلی را داشتند. قبل از رمزنگاری قوی، کاربران برای حفظ امنیت فایل‌های خود باید از پسورد استفاده می‌کردند.

سپس رمزنگاری‌های قوی ایجاد شدند و دردسترس همه قرار گرفتند و نیاز به اعتماد کردن از بین رفت. داده‌ها می‌توانستند به نحوی ایمن شوند که به صورت فیزیکی برای هیچ‌کس قابل دستیابی نباشند، به هر دلیل یا بهانه‌ای که باشد مهم نیست.

حالا زمان آن فرا رسیده است که این اتفاق برای پول نیز رخ دهد؛ با پول الکترونیکی براساس اثبات رمزنگاری، بدون نیاز به اعتماد به شخص سوم و یا یک واسط، به صورت امن و بدون دردسر.

راه حل بیت کوین استفاده از یک شبکه نظیر به نظیر است تا دوبار خرج کردن (Double spending) یک پول را بررسی کند. به طور خلاصه، شبکه شبیه به یک سرور زمان‌سنج توزیع شده کار می‌کند؛ اولین تراکنش برای خرج

کردن یک سکه را برچسب زمانی می‌زند. این ماهیت اطلاعات است که انتشارش را آسان ولی حفظ آن را دشوار می‌کند.

برای جزئیات بیشتر به سایت http://www.bitcoin.org/bitcoin.pdf مراجعه کنید.

زمانی که بیت کوین راه اندازی شد، تعداد انگشت شماری از آن استفاده کردند. آنها شبکه بیت کوین را در کامپیوترهای‌شان (node) اجرا کردند تا شبکه قدرتمندتر شود. بیشتر افراد فکر می‌کردند بیت کوین شبیه به یک جوک است و یا اینکه سیستم بیت کوین نقایص جدی در روند طراحی دارد که آن را غیرقابل اجرا می‌کند.

در طول زمان افراد بیشتری به شبکه بیت کوین پیوستند، از کامپیوترهای‌شان برای افزایش امنیت شبکه استفاده کردند و با مبادله بیت کوین با کالا، خدمات، یا ارزهای دیگر، ارزش بیشتری به آن دادند. امروز، بیش از 10 سال از ارایه بیت کوین می‌گذرد. میلیون‌ها نفر از بیت کوین استفاده می‌کنند، با دهها تا صدها از هزاران گرهی که نرم‌افزار بیت کوین را به صورت رایگان اجرا می‌کنند، که این نرم‌افزار توسط صدها داوطلب و کمپانی در سراسر جهان در حال توسعه است.

بیت کوین اختراعی نبود که بدون هیچ پیش‌زمینه‌ای ساخته شود. در وایت‌پیپری که ساتوشی ارائه داد، به چندین تلاش مهم برای ایجاد سیستم‌های مشابه بیت کوین اشاره شده است، مثل Wei Dai که b-money و Adam Back که hashcash را مطرح کردند. اختراع بیت کوین براساس چنین تلاش‌هایی شکل گرفته است، و در عین‌حال سادگی‌ای که در ایجاد اولین سیستم غیرمتمرکز- که تحت کنترل هیچ شخصی نیست- برای انتقال و صدور پول دیجیتال دارد بسیار قابل توجه است.

بیت کوین چه مشکلی را حل کرده است؟

براساس این کتاب، می‌خواهیم ببینیم چطور نظرات ساتوشی پیاده‌سازی شده‌اند. اگر متوجه مفاهیم ناآشنای این بخش نشدید نگران نباشید، هدف اصلی آشنا شدن با اهداف ساتوشی است. از طریق تمرین و مثال‌های مختلف، این مفاهیم ناآشنا را هم متوجه خواهید شد.

من یک سیستم P2P و open source برای پول الکترونیک ایجاد کرده‌ام

منظور از P2P همان Peer to Peer (نظیر به نظیر یا همتا به همتا) است، به این معنا که در یک سیستم هرکسی می‌تواند بدون هیچ واسطه‌ای با شخص دیگر ارتباط برقرار کند. Napstre، Kazaa و BitTorrent نمونه‌هایی از تکنولوژی P2P برای به اشتراک‌گذاری فایل بودند. BitTorrent برای اولین بار این قابلیت را ارائه داد که بدون دانلود یک موزیک از وبسایت آن را به اشتراک بگذاریم. ساتوشی در طراحی بیت کوین این امکان را ایجاد کرده است که افراد بتوانند پول الکترونیک (e-cash) را بدون واسطه با هم مبادله کنند.

نرم‌افزار، open source (متن باز) است، یعنی هرکسی می‌تواند به کدهای نرم‌افزار دسترسی داشته باشد و چگونگی کارکرد آن را ببیند و حتی تغییراتی در آن ایجاد کند. این مورد از این جهت حائز اهمیت است که حتی نیاز به اعتماد به ساتوشی را هم از بین می‌برد. لازم نیست هرآنچه که ساتوشی در توصیف نرم‌افزار گفته است را باور کنیم، می‌توانیم با بررسی کدها همه چیز را متوجه شویم و اگر چیزی باب میل ما نبود آن را تغییر دهیم.

نرم افزار کاملا غیرمتمرکز است، یک سرور مرکزی یا مراکز معتمد

ساتوشی ذکر می‌کند که سیستم غیرمتمرکز است تا نیاز به مرکز کنترل را از بین ببرد. در تلاش‌های قبل برای ساختن ارز دیجیتال، مثل DigiCash که در سال 1989 توسط David Chaum ارائه شد، یک سرور مرکزی برای پشتیبانی وجود داشت؛ یک یا مجموعه‌ای از کامپیوترها که مسئول تایید پرداخت‌ها و انتشار آنها بودند و توسط یک کمپانی اداره می‌شد.

چنین طرح‌هایی که امکان کنترل مرکزی داشتند محکوم به شکست بودند. افراد نمی‌توانند به پولی اعتماد کنند که درصورتی‌که کمپانی از فعالیت خود دست بکشد، یا هک شود، یا سرورها دچار خرابی شوند و یا دولت آن را تعطیل کند، از بین برود.

ماهیت غیرمتمرکز بیت کوین مفهوم پول نقد را در حوزه دیجیتال بازمی‌گرداند: می‌توان آن را بدون صحبت با کسی انتقال داد، بدون اجازه گرفتن، در تمام طول شبانه روز، تمام 365 روز سال، بدون نیاز به مراجعه به هیچ مرکز معتبری.

همه چیز بر مبنای اثبات رمزنگاری است به جای اعتماد

چگونه بیت کوین نیاز به اعتماد را از بین می‌برد؟ درباره این موضوع در فصل‌های بعد صحبت خواهیم کرد، اما ایده اصلی این است که به جای اعتماد کردن به شخصی که ادعا می‌کند Alice است و یا 10 دلار در حساب بانکی خود دارد، می‌توان از محاسبات رمزنگاری برای اثبات این ادعا استفاده کرد، به نحوی که انجام آن ساده باشد. این قابلیت اساس سیستم بیت کوین است که هم مالکیت پول و هم امنیت شبکه را تامین می‌کند.

درمورد حریم خصوصی باید به بانک‌ها اعتماد کنیم، اعتماد کنیم که به سارقان اجازه نمی‌دهند حساب بانکی ما را خالی کنند

برخلاف حساب‌های بانکی، سیستم‌های پرداخت دیجیتال یا کارت‌های اعتباری، بیت کوین به افراد اجازه می‌دهد بدون ارایه هیچ اطلاعات شخصی با هم دادوستد کنند.

مخازن متمرکزی که اطلاعات مشتریان بانک‌ها، شرکت‌های کارت اعتباری، سیستم‌های پرداخت و دولت‌ها در آن ذخیره می‌شود، برای هکرها بسیار جذاب هستند. هک شدن شرکت اعتباری equifax و قرار گرفتن اطلاعات140 میلیون نفر در دست هکرها گواهی بر این سخن ساتوشی است.

هدف بیت کوین جدا کردن تراکنش‌های مالی از هویت افراد در دنیای واقعی است. وقتی پول نقدی پرداخت می‌کنیم، نیازی نیست طرف مقابل از هویت ما مطلع شود، همچنین جای نگرانی نیست که از اطلاعاتی که به آنها داده‌ایم بتوانند برای سرقت پول بیشتر استفاده کنند.

چرا از ارز دیجیتال همین انتظار و یا حتی بهتر از این را نداشته باشیم؟

باید به بانک مرکزی اعتماد کرد که ارزش پول را حفظ کند، اما سرگذشت پول‌های فیات پر از نقض این اعتماد است

فیات، پولی است که دولت و بانک مرکزی منتشر می‌کنند و توسط دولت به عنوان پول قانونی تعیین شده است. در گذشته پول توسط افراد فعال بازار از بین چیزهایی انتخاب می‌شد که به‌دست آوردن آنها سخت ولی تایید صحت و نیز جابه‌جا کردن آنها آسان بود، مثل نمک، صدف، سنگ، نقره و طلا.

رفته رفته در کل دنیا به‌جای استفاده از طلا به عنوان پول، از یک تکه کاغذ استفاده شد که درواقع گواهی‌کننده وجود طلا بود. درنهایت این تکه کاغذ توسط نیکسون از هرگونه پشتوانه فیزیکی جدا شد و در سال 1971 به تبدیل دلار امریکا به طلا خاتمه داد.

پایان استاندارد طلا، به دولت‌ها و بانک‌های مرکزی اجازه داد تا عرضه پول را به میل خود افزایش دهند. این امر باعث کاهش ارزش اسکناس‌های درگردش شد که تحت عنوان debasement شناخته می‌شود. فیات پولی است که همه ما آن را می‌شناسیم و هرروز از آن استفاده می‌کنیم. اگرچه این پول تحت حمایت دولت است اما پشتوانه ارزشمندی ندارد و درواقع یک مفهوم نسبتا جدید با حدود یک قرن قدمت است.

برخلاف پول فیات که عرضه و ارزش آن قابل پیش‌بینی نیست، ساتوشی نوعی سیستم ارزی را طراحی کرده است که حجم پول در آن ثابت و از قبل مشخص شده و قابل تغییر هم نیست. نهایتا 21 میلیون بیت کوین تولید خواهد شد و هر بیت کوین نیز می‌تواند به 100 میلیون واحد تقسیم شود که به هر واحد آن ساتوشی گفته می‌شود.

قبل از بیت کوین دارایی‌های دیجیتال کم نبودند. در دنیای دیجیتال کپی کردن یک کتاب، فایل صوتی یا ویدیو و ارسال آن به دیگران بسیار ساده است، ولی دارایی‌های دیجیتالی که توسط یک واسطه کنترل می‌شود مستثنی هستند و نمی‌توان آنها را کپی یا ارسال کرد. برای مثال وقتی فیلمی را از iTunes اجاره می‌کنید فقط و فقط در دستگاه شما قابل پخش است؛ چراکه iTunes این مسئله را کنترل می‌کند و می‌تواند با اتمام زمان اجاره‌ی شما پخش آن را متوقف کند. به طور مشابه پول دیجیتال شما هم توسط بانک کنترل می‌شود. این وظیفه بانک است که مقدار پول شما را ثبت کند و درصورت انتقال به شخص دیگر تراکنش را تایید یا رد کند.

بیت کوین اولین شبکه دیجیتالی است که بر نبود هیچ واسطه‌ای تاکید دارد و سرمایه‌ای شناخته‌شده برای انسان است که حجم آن قابل تغییر نبوده و عرضه آن کاملا برنامه‌ریزی‌شده است.حتی فلزات گرانبهایی مانند طلا نیز این قابلیت را ندارند؛ چراکه می‌توانیم ذخایر طلای بیشتر و بیشتری را با نرخ غیرقابل پیش‌بینی استخراج کنیم. در قسمت‌های بعد به چگونگی این موضوع خواهیم پرداخت.

داده‌ها می‌توانند به نحوی ایمن شوند که دسترسی فیزیکی به آن برای هیچکس ممکن نباشد؛ حالا زمان چنین چیزی برای پول فرا رسیده است.

سیستمی که در حال حاظر برای امنیت پول وجود دارد، مثل سپرده‌گذاری در بانک، براساس اعتماد به شخص دیگری است که این کار را انجام می‌دهد. در اعتماد به چنین واسطه‌ای نه تنها باید اطمینان داشته باشیم که کار اشتباه و یا نادرستی توسط واسط انجام نمی‌شود و هکرها سرمایه‌مان را نمی‌دزدند، بلکه باید مطمئن باشیم که دولت نیز پول ما را ضبط یا مسدود نخواهد کرد. با این وجود در سراسر جهان بارها و بارها دیده شده است که دولت‌ها اگر احساس خطر کنند می‌توانند مانع دسترسی افراد به پول خود شوند.

برای فردی که در امریکا یا در یک اقتصاد قانونمند زندگی می‌کند شاید احمقانه به نظر برسد که با فکر اینکه پول خود را از دست داده است بیدار شود. به عنوان مثال پول من به علت عدم استفاده از حساب PayPal به مدت یک‌ماه مسدود شد و حدود یک هفته زمان برد تا بتوانم به پول خودم دسترسی پیدا کنم. من خوش‌شانس هستم

که در ایالات متحده زندگی می‌کنم؛ چراکه یکی از معدود کشورهایی است که حداقل می‌توانم امیدوار باشم اگر paypal پول من را مسدود کند، می‌شود به یک مرجع قانونی مراجعه کرد و همینطور به دولت و بانک اطمینان داشت که پول کسی را سرقت نمی‌کنند.

موارد بدتری نیز ممکن است در بعضی کشورها رخ دهد، مثل بستن بانک‌ها در یونان هنگام سقوط ارزش پول، یا بانک‌ها در قبرس با دزدی از مشتریان خود از وثیقه‌ها استفاده می‌کردند، یا دولت هند که اسکناس‌های بانک خاصی را بی‌ارزش اعلام کرد، و یا محدود کردن افراد از دسترسی به سرمایه خود.

شوروی سابق، جایی که من بزرگ شدم، دارای یک اقتصاد به‌شدت کنترل‌شده مرکزی بود. زمانی که می‌خواستیم آنجا را ترک کنیم هرنفر تنها می‌توانست مقدار محدودی پول را با نرخ ارز رسمی‌ای که دولت تعیین کرده بود و کاملا متفاوت از نرخ واقعی در بازار آزاد بود، تبدیل کند.

بیت کوین سیستمی را ایجاد کرده است که برای حفظ امنیت پول نیازی به اعتماد به شخص سوم وجود ندارد و به جای آن از طریق کلیدهای خاصی که تنها در اختیار شما قرار می‌دهد از دسترسی هرشخص دیگری به کوین‌های شما جلوگیری می‌کند.

بیت کوین پول را از دولت جدا می‌کند و باعث می‌شود دولت‌ها نتوانند دارایی افراد را کنترل کنند.

راه حل بیت کوین، استفاده از یک شبکه نظیر به نظیر است تا دوبار خرج شدن (Double spending) یک پول را بررسی کند. مثل یک سرور زمان‌سنج توزیع‌شده، به اولین تراکنش برای پرداخت یک کوین برچسب زمانی می‌زند.

یک شبکه به مجموعه‌ای از کامپیوترها گفته می‌شود که به هم متصل شده‌اند و می‌توانند به یکدیگر پیام ارسال کنند. کلمه توزیع‌شده به این معنا است که بدون وجود یک کنترل مرکزی تمامی اعضای شبکه با هم در تعامل هستند تا یک شبکه موفق را ایجاد کنند.

در یک سیستم بدون کنترل مرکزی، اطمینان از اینکه هیچ‌یک از اعضا تقلب نمی‌کنند حائز اهمیت است. اصطلاح Double spending به این معنا است که یک سکه توسط یک فرد دوبار خرج شود. ساتوشی می‌گوید برای

پیشگیری از این اتفاق، اعضای شبکه بیت کوین با هم همکاری می‌کنند تا تراکنش‌ها را برچسب زمانی بزنند (به این معنا که براساس زمانی که اتفاق افتاده‌اند مرتب شوند). با این روش می‌توانیم بفهمیم کدام تراکنش اول انجام شده است و از جعل پول جلوگیری می‌شود. در فصل بعد این سیستم را از ابتدا بررسی خواهیم کرد. سیستم این قابلیت را دارد که بدون نیاز به هیچ مرکزی برای اعتبارسنجی، تراکنش‌های جعلی شناخته شوند.

اختراع بیت کوین باعث شده شماری از مشکلاتی که در زمینه حریم خصوصی، کاهش ارزش پول و کنترل مرکزی در سیستم پولی حاضر وجود دارد، حل شود:

1. چگونه یک شبکه نظیر به نظیر ایجاد کنیم که هرکس بتواند داوطلبانه به آن متصل و عضوی از آن شود.
2. چگونه یک گروه از افراد که یکدیگر را نمی‌شناسند یا اعتمادی به هم ندارند می‌توانند اطلاعات ارزشمندی را با هم به اشتراک بگذارند؛ چراکه بین آنها افراد خرابکار نیز ممکن است وجود داشته باشد.
3. چطور بدون وجود یک واسطه، یک شبکه با عملکرد صحیح خواهیم داشت.
4. چگونه یک دارایی دیجیتال ایجاد کنیم که قابل جعل کردن نباشد، سریع تایید شود و در برابر هک و سرقت مقاوم باشد.

بیایید فکر کنیم چطور چنین سیستمی می‌توان ساخت.

فصل دوم: حذف واسطه‌ها

در فصل قبل گفته شد که بیت کوین یک سیستم نظیر به نظیر برای انتقال پول است. قبل از اینکه این مورد را بررسی کنیم، گذری بر نحوه عملکرد بانک‌های سنتی و سیستم‌های پرداخت در بررسی مالکیت و انتقال پول داشته باشیم .

بانک‌ها فقط یک دفترکل هستند

یک سیستم پرداخت که توسط بانک یا Paypal ویا Apple Pay ساخته شده است، چگونه کار می‌کند؟ خیلی ساده؛ واسطه یک دفترکل حاوی اطلاعات حساب‌ها و نقل و انتقالات آنها را دردست دارد.

در این مثال از لفظ بانک استفاده می‌شود ولی منظور هرنوع سیستم پرداخت است. با یک دفترکل (لجر) که حاوی اطلاعات سپرده پولی Alice و Bob در بانک است شروع می‌کنیم.

دفترکل بانک

1. Alice: اعتبار سپرده نقدی +$2
2. Bob: اعتبار سپرده نقدی +$10
3. Alice: برداشت -$2
4. Bob: واریز +$2

بانک تمامی واریزها و برداشت‌ها را ثبت می‌کند و به همین سادگی پول جابه‌جا می‌شود.

تصویر 2: سیستم متمرکز

مشکل double spending

حال اگر Alice تلاش کند تا همان $2 را مجددا خرج کند چه اتفاقی می‌افتد؟ به این اتفاق Double spending گفته می‌شود. Alice درخواست خود را به بانک ارسال می‌کند، اما بانک می‌گوید: "شما قبلا $2 را به Bob پرداخت کرده‌اید و پولی برای ارسال وجود ندارد."

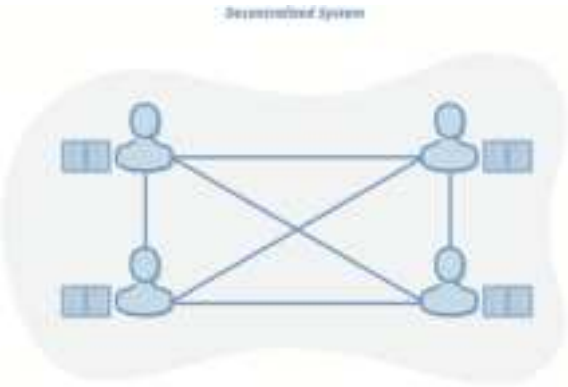
وقتی یک مرجع مرکزی مثل بانک وجود دارد، برای بانک بسیار ساده است که بگوید پولی را که قصد برداشت آن را دارید قبلا برداشت شده است؛ چراکه بانک تنها مرجعی است که دفترکل را ویرایش می‌کند، همچنین بانک‌ها در سیستم داخلی خود دارای سیستم‌های پشتیبان‌گیری و حسابرسی دستی و کامپیوتری هستند تا اطمینان حاصل شود که اطلاعات درست بوده و دستکاری نشده‌اند. به چنین سیستم‌هایی متمرکز گفته می‌شود؛ چراکه تنها یک نقطه کنترل دارد.

دفترکل غیرمتمرکز

اولین مشکلی که بیت کوین قصد حل کردن آن را دارد حذف واسطه‌ی مورد اطمینان با استفاده از یک شبکه نظیر به نظیر است. تصور کنید که بانک‌ها از بین رفته‌اند و ما باید سیستم مالی خودمان را ایجاد کنیم اما این‌بار قرار نیست متمرکز باشد. چگونه بدون یک مرجع مرکزی می‌توان دفترکل را ایجاد کرد؟

اگر دفترکل یک نگه‌دارنده مرجع نداشته باشد، باید در اختیار همه قرار بگیرد. این همان راه ایجاد یک دفترکل غیرمتمرکز است.

ابتدا تعدادی از ما کنار هم جمع می‌شویم و یک شبکه ایجاد می‌کنیم، به این معنا که راهی برای ارتباط با هم داریم. درواقع شماره تماس و حساب Snapchat را با هم ردوبدل می‌کنیم. وقتی Alice قصد دارد پولی برای Bob ارسال کند، به‌جای تماس با بانک، در snapchat به همه دوستان خود می‌گوید: "من $2 برای Bob ارسال می‌کنم." همه تصدیق می‌کنند که این پیغام را دیده‌اند و پاسخ می‌دهند: "بله، ما پیغام را گرفتیم" و در کپی که از لجر نزد خود دارند این جابه‌جایی را یادداشت می‌کنند. حالا تصویر به شکل زیر خواهد بود:



تصویر 3: سیستم غیرمتمرکز

اکنون به‌جای تنها یک دفترکل در بانک، یک کپی از دفترکل دردست هر یک از اعضای شبکه وجود دارد. هر زمانی که کسی قصد خرج کردن پول خود را داشته باشد، به آسانی به همه دوستان خود در snapchat اطلاع می‌دهد و یا تماس گرفته و آنها را مطلع می‌کند. همه این تراکنش را ثبت می‌کنند. به دلیل اینکه دفترکل دیگر تنها در یک مکان مرجع نیست به آن توزیع‌شده می‌گوییم، و چون مرجع مرکزی مسئول آن نیست، به آن غیرمتمرکز گفته می‌شود.

این سیستم چگونه مشکل double spendig را حل می‌کند؟ از آنجایی که همه افراد شبکه یک کپی از لجر نزد خود دارند، اگر Alice بخواهد آن 2 دلاری را که برای Bob ارسال کرده است را دوباره خرج کند، این تراکنش توسط همه در شبکه رد می‌شود؛ چراکه هرکس لجر خود را بررسی می‌کند و به Alice می‌گوید براساس چیزی که ثبت شده او قبلا این پول را خرج کرده است.

اکنون ما یک شبکه نظیر به نظیر داریم که مالکیت و نقل‌وانتقالات مالی را ثبت می‌کند. این سیستم بین گروهی از دوستان که به دلایل اجتماعی یکدیگر را فریب نمی‌دهند بسیار خوب عمل می‌کند، اما در مقیاس بزرگتر اینطور نیست. هرچه تعداد بیشتری از افراد شروع به استفاده از سیستم کنند، احتمال تقلب بیشتر می‌شود.

چطور همه را صادق نگه داریم؟

فصل سوم: بدون نیاز به اعتماد و مجوز

تا زمانی که پیوستن به لجر توزیع‌شده‌ی ما نیازمند اجازه گرفتن باشد و ما بتوانیم به صداقت همه اعتماد کنیم این سیستم به درستی عمل خواهد کرد. اما این طرح برای استفاده میلیون‌ها نفر در سراسر جهان مقیاس‌پذیر نیست.

سیستم‌های توزیع‌شده‌ای که با اعضای تصادفی و شناخته‌نشده ایجاد شده‌اند ذاتا قابل اعتماد نیستند. بعضی از اعضا ممکن است گاهی آنلاین نباشند، و این به معنای این است که اگر تراکنشی در شبکه انجام شود آنها مطلع نخواهند شد. برخی دیگر ممکن است با تصدیق اینکه تراکنشی انجام شده یا نشده است، به دنبال فریب ما باشند. ممکن است افراد جدیدی به شبکه بپیوندند و کپی‌های متناقضی از لجر را دریافت کنند. بیایید بررسی کنیم که یک فرد چگونه می‌تواند تقلب کند.

حمله Double Spend

اگر من Alice باشم، می‌توانم با گروهی از اعضا تبانی کنم و به آنها بگویم: "زمانی که من پولی را خرج می‌کنم آن را در لجر خود ثبت نکنید؛ وانمود کنید که هرگز اتفاق نیفتاده است". به این شکل Alice می‌تواند یک حمله Double Spend انجام دهد. با موجودی 2 دلار Alice به این صورت عمل می‌کند:

1. او 2 دلار خود را برای خرید آب‌نبات به Bob انتقال می‌دهد. حالا باید موجودی وی صفر باشد.

2. David، Eve و Farrah با Alice تبانی کرده‌اند و تراکنش Alice به Bob را در لجر خود ثبت نمی‌کنند. در کپی‌ای که نزد آنهاست Alice هرگز چیزی به Bob پرداخت نکرده است.

3. Charlotte یک فرد قابل اعتماد است که یک کپی از لجر را دارد. او تراکنش Alice به Bob را ثبت می‌کند و حالا در لجرش موجودی Alice صفر است.

4. Henry یک‌هفته در تعطیلات بوده است و از هیچ‌یک از تراکنش‌ها اطلاعی ندارد. او به شبکه متصل می‌شود و تقاضای یک کپی از لجر را می‌کند.

5. Henry چهار کپی نادرست (David,Eve,Farrah,Alice) و یک کپی درست (Charlotte) دریافت می‌کند. چطور متوجه شود که کدام یک درست است؟ چون سیستم بهتری وجود ندارد، به آنچه که در اکثریت لجرها وجود دارد اعتماد می‌کند و کپی نادرست را به عنوان کپی صحیح قبول می‌کند.

6. Alice یک آب‌نبات از Henry می‌خرد و از آن دو دلاری که درواقع ندارد استفاده می‌کند. Henry می‌پذیرد چراکه براساس دانسته‌هایش Alice هنوز 2 دلار در حساب خود دارد (براساس لجری که از دیگران گرفته است).

7. حالا Alice دو آب‌نبات دارد و 4 دلار جعلی در سیستم ایجاد کرده است. او برای این آب‌نبات‌ها به نحوی برای دوستان خود جبران می‌کند، و آنها نیز این حمله را صدها بار برای هرشخص جدیدی که به شبکه متصل می‌شود، تکرار می‌کنند.

8. حالا Alice همه آب‌نبات‌ها را دردست دارد و بقیه افراد نیز کیف‌های بزرگی از پول جعلی.

9. افرادی که به ظاهر پولی را از Alice دریافت کرده‌اند، وقتی بخواهند آن را خرج کنند، David,Eva و Farrah که کنترل بیشتر شبکه را در اختیار دارند، این تراکنش را رد می‌کنند چون می‌دانند که پول از ابتدا جعلی است.

مشکلی که وجود دارد عدم *اجماع* است. افراد در یک شبکه درمورد وضعیت شبکه به اجماع نرسیده‌اند؛ چراکه سیستم بهتری ندارند و از قانون اکثریت پیروی می‌کنند. درحالی‌که اکثریت افرادی که کنترل شبکه را دردست دارند متقلب هستند و پولی را که ندارند پرداخت می‌کنند.

اگر بخواهیم یک سیستم بدون نیاز به مجوز داشته باشیم که هرکسی بتواند عضو آن شود، پس باید در برابر افراد سودجو و متقلب انعطاف‌پذیر باشد.

حل مشکل اجماع غیرمتمرکز

حالا باید یکی از سخت‌ترین مشکلات در علم کامپیوتر را حل کنیم: اجماع غیرمتمرکز بین افرادی که بعضی از آنها خرابکار و غیرقابل اعتماد هستند. این مشکل تحت عنوان فرماندهان بیزانسی شناخته می‌شود و اصلی‌ترین چیزی‌ست که ساتوشی در اختراع بیت کوین از آن استفاده کرده است. بیایید این موضوع را بررسی کنیم.

ما باید گروهی از افراد را درمورد ورودی‌های لجر به توافق برسانیم، بدون اینکه بدانیم دارنده کدام لجر تمام تراکنش‌ها را به درستی ثبت کرده است. یک راه حل ساده‌لوحانه این است که یک فرد مورد اعتماد را برای نگهداری از لجر تعیین کنیم. به‌جای اینکه همه‌ی اعضا تراکنش‌ها را ثبت کنند، تعداد انگشت‌شماری از دوستان مورد اعتماد را انتخاب کنیم، مثل Charlotte,Gary,Frank و Zoe تا آنها تمام تراکنش‌ها را ثبت کنند. بنابراین هر زمانی که بخواهیم تراکنشی انجام دهیم به‌جای اطلاع‌رسانی به همه دوستان‌مان، فقط به Charlotte و باندش خبر می‌دهیم. آنها در ازای دستمزد کمی، این کار را انجام می‌دهند. بعد از اینکه آنها تراکنش را ثبت کردند با همه اعضایی که لجر را به عنوان پشتیبان نگهداری می‌کنند، تماس می‌گیرند و درباره ورودی جدید لجر اطلاع‌رسانی می‌کنند.

این سیستم به خوبی کار می‌کند، مگر زمانی که نمایندگان دولت حاضر شوند و درمورد اداره‌کنندگان این سیستم مالی کنکاش کنند. اگر آنها Charlotte و دوستانش را دستگیر کنند، این پایانی برای لجر غیرمتمرکز ما خواهد شد. نسخه پشتیبان همه ما دیگر غیرقابل اعتماد خواهد بود و به یکدیگر نیز نمی‌توانیم اعتماد کنیم و نمی‌شود فهمید از نسخه پشتیبان کدامیک برای شروع دوباره سیستم می‌تواند استفاده شود.

به‌جای تعطیلی کامل، دولت می‌تواند نگه‌دارندگان لجر را تهدید کند که درصورت پذیرش تراکنش‌های Alice (که مشکوک به فروش مواد مخدر است) آنها را زندانی خواهد کرد. این سیستم نیز به‌شدت تحت کنترل مرکزی است و نمی‌توان آن را بدون نیاز به مجوز خواند.

اگر دموکراسی را امتحان کنیم چه می‌شود؟ یک جمع 50 نفره از افراد قابل اعتماد را مشخص می‌کنیم، و هر روز یک انتخابات برگزار می‌شود که کدامیک تراکنش‌ها را در لجر ثبت کند تا چرخه ادامه یابد. هر عضو شبکه یک رای خواهد داشت.

این سیستم تا زمانی خوب کار می‌کند که کسی آن را افشا نکند؛ در غیر این صورت با تهدید و خشونت پایانی مانند سیستم قبل خواهد داشت:

1. تهدید رای‌دهندگان برای انتخاب فرد مورد نظر دولت
2. تهدید رای‌آورندگان برای ثبت ورودی‌های جعلی در لجر

مشکل این است که، وقتی شخص خاصی برای نگهداری از لجر تعیین می‌شود، باید صادق و قابل اعتماد باشد و دربرابر کسانی که آنها را مجبور به انجام کارهای نادرست در لجر ما می‌کنند، راهی برای دفاع نداریم.

هویت جعلی و حمله Sybil

تاکنون دو روش ناموفق برای اطمینان به شبکه را بررسی کردیم: استفاده از افراد شناخته شده برای نگهداری از لجر، و دیگری انتخاب گزینشی و چرخشی نگه‌دارندگان لجر. شکست هردو سیستم به این دلیل بود که اساس اعتماد ما، به هویت افراد در دنیای واقعی گره خورده بود: هنوز هم مجبور بودیم که افراد را به طور خاص برای نگهداری از لجر شناسایی کنیم.

هروقت اعتماد بر پایه هویت افراد باشد ما خود را در معرض حمله Sybil قرار خواهیم داد. این اسم درواقع یک اصطلاح برای جعل هویت است؛ و نام زنی است که دچار اختلال چندشخصیتی بود.

آیا تابه‌حال یک پیام عجیب از دوستی دریافت کرده‌اید و بعد متوجه شوید که گوشی او توسط برادرش ربوده شده بود؟ وقتی صحبت از میلیون‌ها و یا حتی میلیاردها دلار باشد، هرکسی ممکن است برای دزدیدن و ارسال آن پیام

دست به هرنوع تقلب و خشونتی بزند. برای همین، محافظت از افرادی که لجر را برای ما نگهداری می‌کنند، در برابر تهدیدها، بسیار بااهمیت است. اما چطور؟

بیایید یک قرعه‌کشی ترتیب دهیم

اگر نخواهیم کسی در معرض تهدید به خشونت و رشوه قرار بگیرد، به سیستمی نیاز داریم که تعداد اعضای آن زیاد باشد، در این صورت هیچ‌کس نمی‌تواند آنها را تحت فشار قرار دهد. باید به گونه‌ای باشد که هرکسی بتواند در سیستم عضو شود و هیچ نوع رای‌گیری وجود نداشته باشد؛ چراکه در روش رای‌گیری مشکلات خرید رای افراد و اعمال خشونت و تهدید برای تغییر رای آنها وجود دارد.

اگر یک قرعه‌کشی ترتیب دهیم و هربار یک شخص تصادفی را انتخاب کنیم چه؟ این اولین پیش‌نویس طرح است:

هرکسی در دنیا می‌تواند عضو سیستم باشد. ده‌ها هزار نفر می‌توانند به قرعه‌کشی نگه‌دارندگان لجر در شبکه بپیوندند.

1. زمانی که قصد ارسال پول داریم تمام شبکه را از این امر مطلع می‌کنیم، همان‌طور که قبلا بود.
2. هر 10 دقیقه یک برنده انتخاب می‌شود.
3. زمانی که برنده انتخاب شد، آن شخص باید تمام تراکنش‌هایی را که اتفاق می‌افتد در لجر ثبت کند.
4. اگر شخص برنده یک تراکنش معتبر را در لجر ثبت کند (اگر سایر اعضا نیز اعتبار آن را تایید کنند) مبلغی به عنوان پاداش به او تعلق می‌گیرد.
5. هرکس یک کپی از لجر نزد خود دارد که اطلاعاتی که برنده قرعه‌کشی ارایه می‌دهد را در آن ثبت می‌کند.
6. مدت زمان قرعه‌کشی 10 دقیقه تعیین شده است تا مطمئن شویم افراد، زمان کافی برای به‌روزرسانی لجر خود دارند.

این سیستم پیشرفته‌تر است؛ چراکه به دلیل نامشخص بودن برنده بعدی، زدوبند با اعضای سیستم ممکن نیست.

اما باز هم اشکالاتی وجود دارد. چه اشکالاتی؟

سیستم خودکار قرعه‌کشی

این سیستم قرعه‌کشی دو مشکل اساسی دارد:

1. چه کسی بلیط قرعه‌کشی را می‌فروشد و برنده را انتخاب می‌کند، درحالی‌که ما مشخص کرده‌ایم نباید هیچ نوع موجودیت مرکزی وجود داشته باشد تا اجرای قرعه‌کشی به خطر نیفتد.
2. چطور مطمئن شویم که برنده قرعه‌کشی واقعا تراکنش‌های درست را در لجر ثبت کرده است و قصد گمراه کردن بقیه ما را ندارد؟

اگر می‌خواهیم یک سیستم بدون نیاز به مجوز داشته باشیم که همه بتوانند به آن بپیوندند، باید نیاز به اعتماد را در سیستم از بین ببریم و در اصلاح، سیستم Trustless باشد. باید سیستمی را ارائه دهیم که این ویژگی‌ها را داشته باشد:

1. برای همه اعضا باید این امکان وجود داشته باشد که شخصا بلیط قرعه‌کشیِ خودشان را ایجاد کنند، چون به هیچ مرجعی نمی‌توان اعتماد کرد.
2. بقیه اعضا باید به سادگی بتوانند با بررسی بلیط، صحت برنده شدن شما در قرعه‌کشی را تشخیص دهند، چون به کسی نمی‌توان برای تعیین برنده‌ی رقابت اعتماد کرد.
3. اگر کسی برنده قرعه‌کشی شد و تراکنش نامعتبری را در لجر ثبت کرد، باید تنبیه شود. به‌جای اعتماد به افراد خاص در شبکه، با استفاده از شیوه تنبیه و تشویق، اعتماد را در شبکه نهادینه کنیم .

بیایید تک تک این موارد را حل کنیم. توضیح چگونگی انجام این قرعه‌کشی شاید سخت‌ترین چیز در فهمیدن بیت کوین باشد. به همین دلیل، 3 فصل بعدی را برای بررسی عمیق این مسئله درنظر گرفته‌ایم.

سیستم مرکزی استاندارد قرعه‌کشی مثل بخت‌آزمایی توسط یک فرد اجرا می‌شود که به‌صورت تصادفی مجموعه‌ای از اعداد و تعدادی بلیط با شماره‌های تصادفی تولید می‌کند. تنها شماره یک بلیط مشابه شماره‌ای است که توسط سازمان اداره‌کننده بخت‌آزمایی به شکل محرمانه تولید شده است. اما از آنجایی که ما نمی‌توانیم به هیچ مرجعی اعتماد کنیم باید اجازه دهیم هر فرد خودش اعداد تصادفی خود را تولید کند.

چطور برنده را تشخیص دهیم؟ در بخت‌آزمایی مسئولانِ آن از ترکیب برنده مطلع هستند. چون ما نمی‌توانیم چنین شخصی را در سیستم غیرمتمرکز داشته باشیم، درعوض می‌توانیم سیستمی را ایجاد کنیم که همه بتوانند از قبل درباره یک بازه عددی به توافق برسند. اگر عدد تصادفی شما در این بازه قرار گرفت شما برنده هستید. ما از یک روش رمزنگاری به نام Hash برای این کار استفاده می‌کنیم. در فصل 4 درباره hash مفصل صحبت خواهیم کرد.

درنهایت باید راهی برای تنبیه افراد متقلب داشته باشیم. تولید اعداد تصادفی، مثل بلیط بخت‌آزمایی، اساسا رایگان است. چطور این را به گونه‌ای ارائه دهیم که شما ملزم به پرداخت وجه برای خرید بلیط شوید درحالی‌که کسی وجود ندارد که از او بلیط بخرید؟ شما باید این بلیط را با هزینه کردن از انرژی دنیا بخرید؛ منبع کمیابی که از چیزی به وجود نمی‌آید. در فصل 5 این ایده شرح داده خواهد شد.

اثبات کار: یک معمای سخت

راه حل مناسب برای این سه مشکل، اثبات کار (proof of work) است. این روش قبل از اختراع بیت کوین در سال 1993 مطرح شد.

قیمت بلیط قرعه‌کشی باید زیاد باشد وگرنه افراد، تعداد نامحدودی شماره بلیط تولید می‌کنند. چه چیزی به این اندازه قیمت دارد اما در مرکز معتبری عرضه نمی‌شود؟

در ابتدای کتاب، اشاره به نقش فیزیک و علوم دیگر در ساخت بیت کوین کردم و اینجا همان نقطه‌ای است که فیزیک در بیت کوین نقشی ایفا می‌کند: اولین قانون ترمودینامیک می‌گوید انرژی نه به‌وجود می‌آید و نه از بین می‌رود. به بیان دیگر انرژی چیزی مثل غذای رایگان نیست. انرژی برق همیشه گران است چون یک انرژی کمیاب و هزینه‌بر است. برق را یا باید از تولیدکنندگان آن بخرید یا نیروگاه خودتان را راه‌اندازی کنید. در هرصورت شما نمی‌توانید چیزی را از هیچ به وجود آورید.

مفهوم پشت Proof of work این است که، شما در یک فرایند تصادفی شرکت می‌کنید، مثل پرتاب تاس، اما به‌جای شش وجه، تاس ما به اندازه اتم‌های جهان وجه دارد. برای پرتاب تاس و تولید اعداد قرعه‌کشی، کامپیوتر شما باید عملیات زیادی را انجام دهد که نیازمند صرف انرژی برق است.

برای برنده‌شدن در قرعه‌کشی باید یک عدد خاص را تولید کنید که به لحاظ محاسباتی آن عدد از "تراکنشی که قرار است در لجر ثبت شود" و "یک عدد تصادفی"، به‌دست می آید (جزئیات عملکرد این موضوع در فصل آینده بررسی خواهد شد).

برای رسیدن به این عدد برنده، ممکن است مجبور شوید تاس را میلیون‌ها، میلیاردها و یا حتی بیشتر پرتاب و صدها یا هزاران دلار برای صرف انرژی هزینه کنید. چون این فرایند براساس تصادف است، برای همه این امکان وجود دارد که بلیط قرعه‌کشی خود را تولید کنند؛ با استفاده از یک سخت‌افزار یا نرم‌افزار و یک لیست از تراکنش‌هایی که باید در لجر ثبت شود و بدون نیاز به یک مرجع مرکزی می‌توانند اعداد تصادفی تولید کنند.

حتی اگر هزاران دلار برای پیدا کردن عددِ درست انرژی مصرف کرده باشید، بقیه افراد شبکه برای اینکه تایید کنند شما برنده هستید باید به دو بررسی اساسی بپردازند:

1. عددی که شما تولید کرده‌اید از آستانه‌ای که همه درمورد آن توافق کرده‌اند کوچکتر است یا بزرگتر؟

2. آیا این عدد از نظر ریاضی به راستی از مجموعه‌ای از تراکنش‌های معتبر که می‌خواهید در لجر ثبت کنید به‌دست آمده است؟

این فرایند سیستم Proof of work را یک سیستم نامتقارن می‌کند، به این معنا که تولید عدد بسیار سخت ولی اعتبارسنجی آن آسان است.

هزینه زیادی که برای مصرف انرژی در تولید عدد تصادفی پرداخت می‌شود- که همه باید صحت آن را تایید کنند- انگیزه کافی را در افراد ایجاد می‌کند که درست عمل کرده و فقط تراکنش‌های معتبر را در لجر ثبت کنند.

برای مثال اگر تلاش کنید پولی که قبلا صرف شده است را مجددا پرداخت کنید، بلیط برنده شما از طرف همه رد می‌شود، و شما پول زیادی را هم که برای انرژی هزینه کرده‌اید از دست خواهید داد. از طرف دیگر اگر بتوانید تراکنش‌های معتبر را در لجر ثبت کنید، به عنوان پاداش بیت کوین دریافت خواهید کرد تا با آن هزینه انرژی صرف شده را پرداخت و کمی هم سود کنید.

ویژگی Proof of work گران بودن آن در دنیای واقعی است. امروزه تخمین زده می‌شود که میزان مصرف انرژی شبکه بیت کوین برای این قرعه‌کشی از مصرف برق بعضی کشورهای با اندازه متوسط بیشتر است.

اعضای شبکه چطور ثابت می‌کنند که انرژی مصرف کرده‌اند؟ این مورد در فصل بعد بررسی می‌شود.

فصل 4: ریاضیات بیت کوین

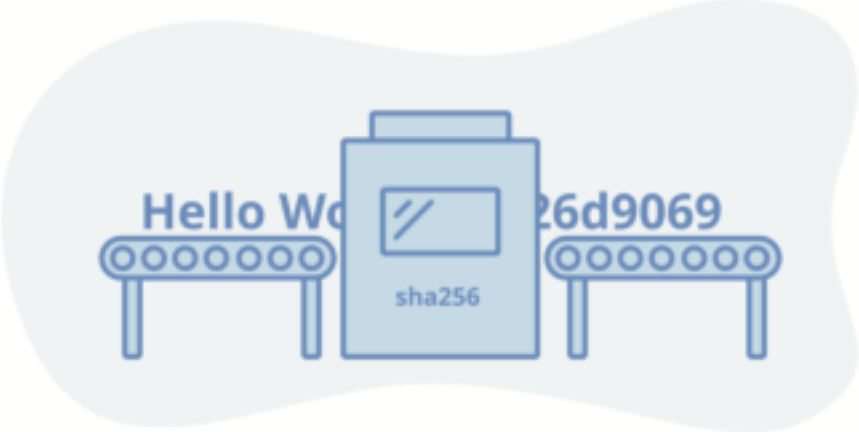
قبل از اینکه درمورد چگونگی ارزیابی proof of work بحث کنیم، نیاز به اطلاعات مختصری از علم کامپیوتر داریم: بیت و Hashing

Hashing

معمای Proof of work در بیت کوین وابسته به استفاده از یک تابع hash است. می‌دانیم که یک تابع مثل جعبه‌ای است که اگر مقدار X را به‌عنوان ورودی به آن بدهید، مقدار خروجی Y را از آن دریافت می‌کنید. مثلا تابع f(x)=2x یک مقدار را می‌گیرد و در عدد 2 ضرب می‌کند. اگر ورودی 2 باشد خروجیِ تابع 4 خواهد بود.

تابع هش یک تابع خاص است که هر رشته‌ای از حروف، اعداد یا داده‌ای را دریافت کند، خروجی آن یک عدد تصادفی بزرگ خواهد بود.

“Hello world”:
1111811713258219242661329357757490458455489044664361600112658434663354
1502095
من از تابع هشی به نام sha256 برای هش کردن Hello word استفاده کرده‌ام که در بیت کوین نیز استفاده می‌شود.



تابع sha256 ویژگی‌هایی دارد که برای ما مناسب است:

1. خروجی آن قطعی است: برای یک ورودی ثابت همیشه یک خروجی ثابت دارد
2. خروجی آن غیرقابل پیش‌بینی است: تغییر حتی یک کاراکتر و یا اضافه کردن فاصله در رشته ورودی، به کلی خروجی را عوض می‌کند به گونه‌ای که نمی‌توانید رابطه‌ای بین ورودی و خروجی پیدا کنید
3. برای هر اندازه‌ای از ورودی زمان محاسبه کوتاه است
4. این تقریبا غیرممکن است که دو رشته ورودی متفاوت، خروجی یکسانی داشته باشند
5. از خروجی sha256 نمی‌توان ورودی را به‌دست آورد
6. اندازه خروجی همیشه ثابت است (در sha256 همیشه 256 بیت است)

گذری سریع بر بیت‌ها

سیستم عددی که معمولا می‌شناسید شامل اعداد 0 تا 9 است که به آن سیستم دسیمال (ده دهی) می‌گویند چون 10 رقم دارد. کامپیوترها سیستم عددی متفاوتی دارند که از صفر و یک ساخته شده است، که نشان‌دهنده وجود یا عدم وجود سیگنال الکتریکی است. به این سیستم عددی، باینری(دو دویی) می‌گویند.

در سیستم دسیمال تنها از ارقام 0 تا 9 استفاده می‌شود. اگر بخواهید اعداد یک رقمی ایجاد کنید می‌توانید 10 عدد مختلف داشته باشید از 0 تا 9. اگر بخواهید اعداد دورقمی ایجاد کنید می‌توان 10×10 عدد مختلف تولید کرد از 0 تا 99. برای سه رقم، 10×10×10 عدد قابل تولید است از 0 تا 999.

تصور کنید که با N رقم چه عدد بزرگی را می‌توان تولید کرد. 10 را N بار در خودش ضرب می‌کنیم، به عبارت دیگر 10^N ، 10 به توان N.

سیستم باینری هم به همین شکل کار می‌کند. تنها تفاوت آن تعداد ارقام قابل استفاده است. وقتی در سیستم دسیمال از 10 رقم می‌توان استفاده کرد، در سیستم باینری یا بیتی فقط از دو رقم صفر و یک استفاده می‌شود.

اگر به یک بیت، فقط رقم‌های صفر و یک را نسبت دهیم، با 2 بیت می‌توان 4 مقدار تولید کرد:00,01,10,11

با 3 بیت، 2×2×2 یعنی 8 عدد مختلف می‌توان نشان داد: 000,001,010,011,100,101,110,111.

با N بیت در سیستم باینری 2^N عدد مختلف می‌توان ایجاد کرد.

بنابراین با 256 بیت، اندازه خروجی تابع هش sha256 ، 2^{256} عدد مختلف و غیرتکراری می‌توان ایجاد کرد، که به‌صورت غیرقابل تصوری بزرگ است. در سیستم دسیمال، 2^{256} دارای 78 رقم است، عددی به بزرگی تعداد اتم‌های جهان.

115,792,089,237,316,195,423,570,985,008,687,907,
853,269,984,665,640,564,039,457,584,007,913,129,639,936

این عدد، تعداد خروجی‌های ممکن با استفاده از تابع sha256 است. بنابراین حدس اینکه تابع چه عددی را قرار است تولید کند تقریبا غیرممکن است، مثل پیش‌بینی 256 بار پرتاب یک سکه پشت‌سرهم، یا حدس زدن مکان یک اتم خاص که در جایی از جهان انتخاب کرده‌ایم.
به دلیل بزرگ بودن این عدد برای نوشتن، از این به بعد آن را به‌صورت 2^{256} نشان می‌دهیم که امیدوارم تصویر ذهنی درستی از احتمالات ممکن برای شما ایجاد کند.

بیایید یک رشته را هش کنیم

در اینجا تعدادی رشته و هش sha256 آنها آورده شده‌اند. خروجی آنها به شکل دسیمال نشان داده شده است اما در کامپیوتر این عدد به شکل رشته‌های باینری صفر و یک قرار می‌گیرد. هدف نشان دادن این نکته است که چطور با یک تغییر کوچک در ورودی، عدد خروجی تغییر می‌کند و اینکه نمی‌توان در تابع هش براساس ورودی، خروجی را پیش‌بینی کرد:

"Hello world!"
52740724284578854442640185928423074974
81806529570658746454048816174655413720

"Hello world!!"
95863319874939535731602344194643497258 3
74513872780665335270495834770720452323

برای هیچ‌کس حتی کامپیوترها هم ممکن نیست که بتوانند از خروجی تابع، رشته ورودی آن را پیدا کنند. اگر مایل باشید، در بعضی سایت‌ها امکان کار با sha256 به‌صورت آنلاین نیز وجود دارد.

هش کردن برای برنده شدن در قرعه‌کشی Proof of work

حالا آماده صحبت درباره بیت‌های قرعه‌کشی هستیم. گفته شد که 2^{256} خروجی ممکن برای sha256 وجود دارد. برای درک بهتر بیایید تصور کنیم 1000 خروجی ممکن برای تابع هش وجود دارد. سیستم قرعه‌کشی به صورت زیر عمل خواهد کرد.

1. Alice اعلام می‌کند که می‌خواهد 2 دلار برای Bob ارسال کند.
2. همه برای تراکنش " Alice 2دلار به Bob پرداخت کرده است" در قرعه‌کشی شرکت می‌کنند و یک عدد تصادفی که به آن nonce گفته می‌شود را (عددی که فقط یک بار استفاده می‌شود) به انتهای آن اضافه می‌کنند. این کار بدین منظور است که مطمئن شوند رشته‌ای که هش می‌شود با سایرین متفاوت است و به پیدا کردن شماره برنده قرعه‌کشی نیز کمک می‌کند.

3. اگر عدد به‌دست‌آمده بزرگتر از عددی باشد که درباره آن توافق شده است (عدد هدف)، عملیات هش با nonce دیگری تکرار می‌شود:
" Alice 2دلار به Bob پرداخت کرده است =12345" سپس " Alice 2دلار به Bob پرداخت کرده است =92435"، " Alice 2دلار به Bob پرداخت کرده است =1328490123480921345" و ... تا درنهایت به عددی دست بیابید که از عدد هدف کوچکتر باشد.

ممکن است برای رسیدن به جواب بارها و بارها این عملیات تکرار شود. حالا موضوع این است: اگر 1000 هش ممکن وجود داشته باشد و عدد هدف 100 تعیین شده باشد، چه درصدی از هش‌ها کوچکتر از عدد هدف خواهند بود؟

در 1000 عدد ممکن بین صفر تا 999، 100 عدد وجود دارد که از 100 کوچکتر هستند و 900 عدد دیگر بزرگتر. بنابراین 100/1000 یا 10٪ از هش‌ها کوچکتر از هدف هستند. درنتیجه اگر تمام رشته‌ها را هش کنید و تابع هش شما 1000 خروجی متفاوت داشته باشد، انتظار می‌رود که 10٪ مواقع خروجی‌های شما کوچکتر از 100 باشد.

سیستم قرعه‌کشی به این شکل کار می‌کند: یک عدد هدف مشخص می‌شود، و همه درمورد آن با هم به توافق می‌رسند (قبلا گفته شد که در بیت‌ها به چه شکل است). سپس همه تراکنش‌هایی که افراد دارند را دریافت و آنها را هش می‌کنند. یک مقدار nonce به انتهای آن اضافه می‌شود. به محض اینکه یک نفر هشی را پیدا کند که کوچکتر از هدف باشد، به همه افراد شبکه اعلام می‌شود که:

- من تراکنش‌های " Alice 2 دلار به باب پرداخت کرده است، Charlotte 5 دلار به الیس پرداخت کرده است" را دریافت کردم.
- مقدار nonce 32895 را به انتهای آن اضافه کردم.
- به مقدار هش 42 دست یافته‌ام که کمتر از هدف 100 است.
- این proof of work من است: داده‌های تراکنش، nonce که من اضافه کرده‌ام، و هش تولید شده براساس این ورودی.

این موفقیت حاصل میلیون‌ها بار هش کردن برای رسیدن به خروجی مورد نظر و پرداخت هزاران دلار هزینه‌ی انرژی است، اما همه می‌توانند بلافاصله هش من را ارزیابی کنند، ورودی و خروجی به آنها داده می‌شود و آنها می‌توانند با هش کردن ورودی، صحت خروجی را تایید کنند. به یاد داشته باشید که هش قابلیت تبدیل به ورودی را ندارد اما محاسبه آن ساده است.

این فرایند چگونه در ارتباط با مصرف انرژی است؟ قبلا گفته شد که تعداد هش‌های ممکن، عدد بسیار بزرگی به اندازه اتم‌های جهان است. حالا اگر عدد هدف را کوچک کنیم کسر کمتری از هش‌ها معبتر خواهند بود. به این

معنا است که هرکسی که می‌خواهد یک هش معتبر پیدا کند باید زمان محاسباتی و میزان برق بسیار زیادی را صرف کند تا به هدف برسد.
هرچه عدد هدف کوچکتر باشد تلاش بیشتری برای پیدا کردن عدد مناسب نیاز است، و هرچه عدد هدف بزرگتر باشد با سرعت بالاتری می‌توان هش برنده را پیدا کرد.

فصل5: ماینینگ

حالا آماده‌ایم تا ببینیم proof of work در بیت کوین واقعا چطور کار می‌کند:

1. هرکس در هرجای دنیا که بخواهد می‌تواند با اتصال کامپیوتر خود به شبکه بیت کوین عضوی از آن باشد و تراکنش‌ها را دریافت کند.
2. الیس اعلام می‌کند که قصد دارد تعدادی سکه برای باب ارسال کند. کامپیوترهای شبکه این تراکنش را بین هم پخش می‌کنند تا سراسر شبکه از آن مطلع شود.
3. همه کامپیوترهایی که قصد شرکت در این بخت‌آزمایی را دارند با اضافه کردن مقدار nonce و اجرای تابع sha256، شروع به هش کردن تراکنش دریافتی می‌کنند.
4. اولین کامپیوتری که هشی را پیدا کند که کوچکتر از مقدار هدف باشد برنده این بخت‌آزمایی است.
5. این کامپیوتر، مقدار برنده همچنین مقدار ورودی (تراکنش و مقدار nonce) را اعلام می‌کند. این عمل ممکن است ساعت‌ها و یا فقط چنددقیقه طول بکشد. تمام این اطلاعات درکنار هم (تراکنش، nonce ، مقدار هش proof of work) را یک بلاک می‌گویند.
6. همه اعضا بلاک ایجاد شده را از نظر اینکه آیا تراکنش‌ها و مقدار نانس و هش واقعا درست هستند یا نه بررسی می‌کنند: اینکه هش به‌دست‌آمده واقعا کوچکتر از مقدار هدف است و بلاک هیچ تراکنش نامعتبری ندارد و اینکه تاریخچه این بلاک متناقض با بلاک‌های قبلی نیست.
7. همه اعضا این بلاک را در کپی لجر نزد خود ثبت می‌کنند و بلاک را به انتهای زنجیره بلاک‌هایی که قبلا ثبت شده‌اند اضافه و یک بلاکچین ایجاد می‌کنند.

تمام ماجرا همین است. ما اولین بلاک و اولین ورودی لجر را ایجاد کردیم.
فرایند انجام عملیات proof of work، برنده شدن در آن، و نیز نوشتن بلاک در لجر بیت کوین، عملیات ماینینگ را تشکیل می‌دهند.

بیت کوین‌های جدید چگونه استخراج می‌شوند؟

توضیح دادیم که چگونه الیس 2 دلار به باب ارسال می‌کند. از این به بعد دیگر درباره دلار صحبت نمی‌کنیم، چون بیت کوین چیزی درباره دلار نمی‌داند. چیزی که ما داریم بیت کوین است- یک واحد دیجیتال که بیانگر ارزش در شبکه بیت کوین است.

برای بازبینی مثالی که زده شد، آنچه که دقیقا اتفاق افتاده این است که الیس 2 بیت کوین به حساب باب ارسال می‌کند، درواقع بیت کوینی را که در حساب خود ثبت شده بود در حساب باب ثبت می‌کند، و کسی که برنده قرعه‌کشی Proof of work شود این تراکنش را در لجر ثبت می‌کند.

اما آلیس آن دو بیت کوین را برای شروع از کجا آورده است؟ بیت کوین چگونه شروع به کار کرد و چطور افراد قبل از اینکه جایی برای خرید بیت کوین وجود داشته باشد آن را به دست می آوردند؟

جواب این سوال به فرایند ماینینگ (استخراج) بیت کوین برمی‌گردد، که درواقع فرایند شرکت در proof of work و گرفتن اجازه دسترسی به لجر است؛ این تمام چیزی است که بیت کوین را تولید می‌کند. زمانی که شما اعتبار یک بلاک را تایید می‌کنید (با صرف میزان زیادی انرژی و پیدا کردن عدد برنده)، اجازه ثبت هر تراکنشی که دریافت کرده‌اید را می‌توانید در بلاک و همچنین در لجر ثبت کنید. بجز این می‌توانید یک تراکنش بسیارخاص را هم به بلاک اضافه کنید که به آن تراکنش Coinbase می‌گویند. این تراکنش درواقع می‌گوید: "12.5 بیت کوین استخراج شد و به ماری که یک ماینر است پرداخت می‌شود، بابت هزینه‌ی انرژی صرف شده برای ماین کردن بلاک".

جایزه بلاک

بنابر آنچه گفته شد، کسی که یک بلاک را ماین کند می‌تواند بیت کوین‌های جدیدی برای خود استخراج کند. چرا 12.5 بیت کوین، چرا 1000بیت کوین نه؟ چرا ماری نمی‌تواند تقلب کند و هرمقدار بیت کوینی که دوست دارد برای خود بردارد؟ این قسمت کلیدی است: بیت کوین یک سیستم از اجماع توزیع‌شده است. به این معنا که همه افراد باید درمورد آنچه که معتبر تشخیص داده شده است توافق داشته باشند.

اگر ماری یک بلاک را ماین کند و بخواهد به خودش بیت کوین بیشتری بدهد، کامپیوتر سایر اعضا این بلاک را غیرمعتبر تشخیص خواهد داد؛ چراکه در نرم افزار کاربران بیت کوین که همه آن را اجرا کرده‌اند کدی وجود دارد که اعلام می‌کند: "جایزه این بلاک دقیقا 12.5 بیت کوین است. در صورت مشاهده بلاکی با مقداری بیشتر، آن را قبول نکنید."

اگر ماری تقلب کند و یک بلاک نامعتبر را ایجاد کند، آن بلاک در لجر هیچ‌کس ثبت نخواهد شد و او تنها صدها دلار انرژی به هدر داده است.

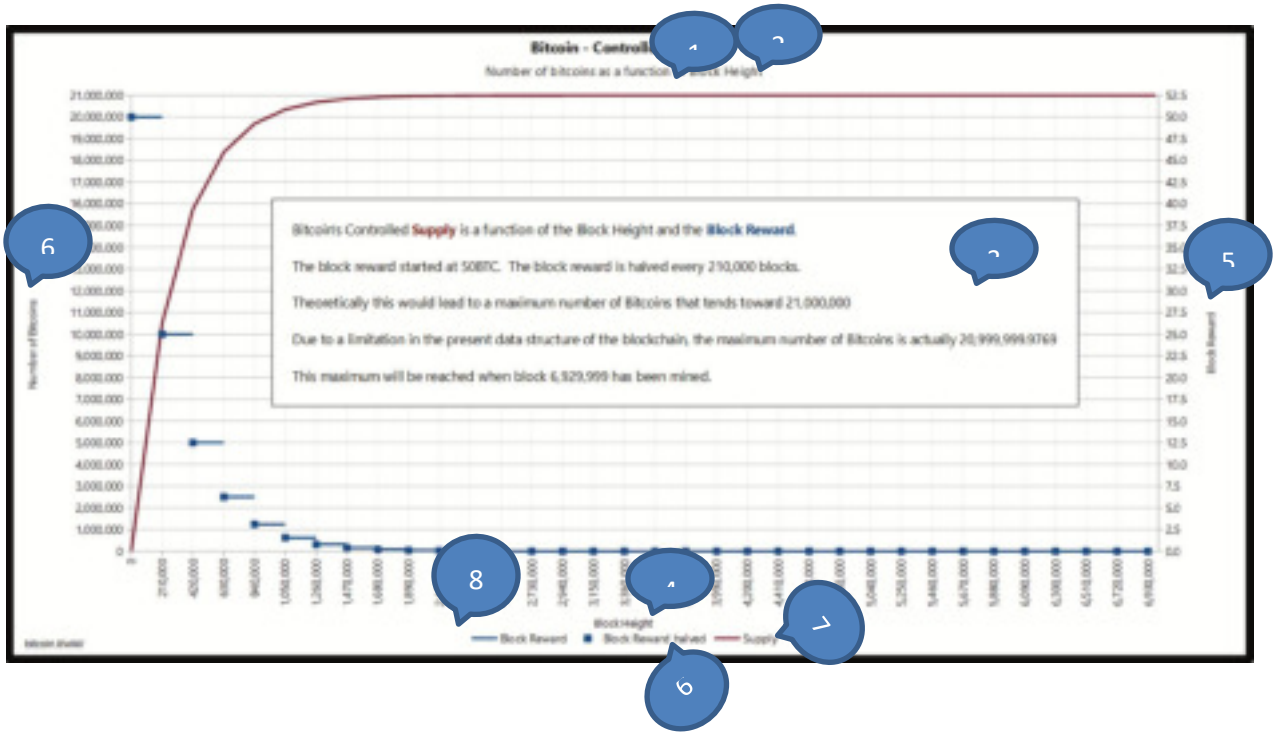
اولین بلاکی که ماین شد، توسط ساتوشی بود. کد آن متن باز است- به معنای اینکه همه می‌توانند آن را ببینند و اعتبارسنجی کنند که هیچ چیز مشکوکی در جریان نیست. حتی ساتوشی هم برای ماین کردن اولین بلاک عملیات proof of work و محاسبات را انجام داده است.

در ابتدا جایزه ماین کردن هر بلاک 50 بیت کوین بود، چیزی که ساتوشی برای ماین کردن اولین بلاک دریافت کرد. زمانی که افراد دیگری در همان روزهای اول به شبکه پیوستند اولین بلاک ماین شده بود.

کدهای بیت کوین هر چهارسال یک بار مقدار جایزه بلاک را نصف می‌کنند (در اصطلاح رایج، هالوینگ گفته می‌شود). این کاهش بیشتر براساس تعداد بلاک‌های ماین شده از ابتدای بیت کوین است نه فقط گذر زمان، چیزی شبیه به تولید بلاک در هر 10 دقیقه.

در سال 2008 جایزه هر بلاک 50 بیت کوین بود، در 2012 معادل 25 بیت کوین و در سال 2016 معادل 12.5 بیت کوین. امروز، 15 ژانویه 2019، تعداد 558668 بلاک از ابتدای تاریخ بیت کوین ماین شده است و جایزه آن 12.5 بیت کوین برای هر بلاک است.

71312 بلاک دیگر، یا تقریبا می سال 2020 مقدار جایزه به 6.25 بیت کوین کاهش می‌یابد، که میزان عرضه بیت کوین را سالانه ٪1.8 افزایش خواهد داد. یک دهه بعد، که دوبار دیگر مقدار جایزه بیت کوین نصف شود، بیشتر از ٪99 تمام بیت کوین‌ها ماین شده است و کمتر از 1 بیت کوین برای تولید هر بلاک پرداخت خواهد شد.



1. کنترل عرضه بیت کوین
2. تعداد بیت کوین‌ها تابعی از تعداد بلاک‌های ماین شده است
3. کنترل عرضه بیت کوین تابعی از تعداد بلاک‌های ماین شده و جایزه هر بلاک است

جایزه بلاک با 50 btc شروع شد و هر 210000 بلاک یک هالوینگ اتفاق افتاد

به صورت تئوری این روند به سمت بیشترین مقدار بیت کوین که 21 میلیون است ادامه پیدا می‌کند به دلیل محدودیت‌هایی که در ساختار بلاکچین در حال حاضر وجود دارد تعداد واقعی بیت کوین‌ها 209999999769 است.

زمانی که بلاک 6929999 ماین شود تمام بیت کوین‌ها استخراج شده‌اند

4. تعداد بلاک‌های ماین شده
5. جایزه ماین کردن هر بلاک
6. تعداد بیت کوین
7. میزان بیتکون عرضه شده
8. جایزه بلاک
9. هالوینگ

درواقع در سال 2140 دیگر جایزه‌ای برای بلاک وجود نخواهد داشت و درآمد ماینرها از دستمزدی است که از ایجادکننده‌های تراکنش دریافت خواهند کرد.

عرضه و جایزه بلاک‌ها در کد بیت کوین- تکرار می‌کنم که کاملا متن باز و برای همه قابل بررسی است- بسیار مهم است، پس با توجه به سابقه‌ای که بیت کوین دارد، تولید بلاکی که برخلاف قوانین بیت کوین باشد ممکن نیست و از طرف همه کسانی که قوانین نوشته شده در کد بیت کوین را کنترل می‌کنند، رد می‌شود.

کنترل فاصله زمانی انتشار و ماین کردن

انجام عملیات ماینینگ نیاز به سخت‌افزار و برق دارد، بنابراین هرچه سخت‌افزار و برق بیشتری داشته باشید، به احتمال بیشتری عدد برنده را سریع‌تر از سایرین پیدا خواهید کرد. برای مثال اگر 100 کامپیوتر مشابه در شبکه وجود داشته باشد و 10 تای آنها متعلق به شما باشد، در این صورت 10٪ مواقع شما برنده خواهید بود. البته، فرایند ماین کردن براساس شانس و تصادف است و گاهی ممکن است ساعت و یا حتی روزها هیچ بلاکی را نتوانید پیدا کنید.

با توجه به بخش‌های قبل می‌دانیم که ماینرها نمی‌توانند جایزه دلخواهی را برای خود تعیین کنند و توسط سایر گره‌های شبکه رد می‌شوند. اما اگر برای تسریع در ماین کردن بلاک‌ها انرژی بیشتری صرف کنند و بیشترین

حجم استخراج بیت کوین در دست آنها باشد چه؟ این نقض محدودیتی است که در قوانین بیت کوین شناخته شده‌اند.

بیایید به مثال برگردیم: تنها 1000 هش ممکن وجود دارد و عدد هدف 100 است؛ به معنی اینکه 10٪ مواقع عددی که تولید می‌شود کوچکتر از 10 است و بلاک پیدا می‌شود. به عبارت دیگر، زمان محاسبه هر هش یک ثانیه است. اگر هرثانیه یک بار تراکنش جاری را با عدد nonce هش کنیم و 10٪ مواقع به عددی کوچکتر از عدد هدف برسیم، به طور میانگین 10 ثانیه زمان برای پیدا کردن هش معتبر نیاز داریم.

حالا اگر دو کامپیوتر برای شرکت در این بخت‌آزمایی باشند چه؟ سرعت دوبرابر می‌شود و انتظار می‌رود در 10 ثانیه هش معتبر پیدا شود. اگر با 10 کامپیوتر این کار را انجام دهیم چه؟ تقریبا هر ثانیه یکی از آنها هش درست را پیدا خواهد کرد.

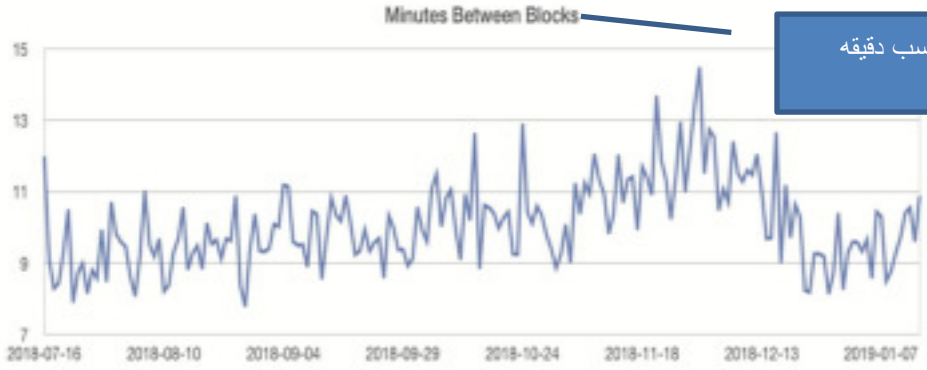
مشکل این است که اگر تعداد افراد بیشتری ماین کنند، بلاک‌ها به سرعت ایجاد خواهند شد، که دو پیامد نامطلوب دارد:

1. باعث اختلال در برنامه ازپیش مشخص‌شده‌ی عرضه بیت کوین می‌شود. ما می‌خواهیم بیت کوین‌هایی که در هرساعت عرضه می‌شوند تعداد نسبتا ثابتی داشته باشند تا اطمینان حاصل شود که تا سال 2140 تمام بیت کوین‌ها عرضه شده‌اند و نه زودتر از آن.
2. باعث ایجاد مشکل در شبکه می‌شود: اگر بلاک‌ها با سرعت بالایی ماین شوند، زمان کافی وجود ندارد که بلاک به‌دست همه افراد شبکه برسد و قبل از اینکه همه از آن مطلع شوند بلاک ماین شده است، بنابراین نمی‌توان درمورد تاریخچه بلاک‌ها به اجماع رسید. مثلا ممکن است که چند ماینر تراکنش یکسانی در بلاک خود داشته باشند و ما قبلا آن تراکنش را در بلاک دیگری ثبت کرده باشیم، که این باعث می‌شود بلاک آنها رد شود.

و اگر تعداد افراد کمتری عمل ماینینگ را انجام دهند برعکس این مشکلات را خواهیم داشت:

1. سرعت شبکه بسیار کم شده و دوباره در عرضه بیت کوین اختلال ایجاد می‌شود.
2. اگر افراد، ساعت‌ها و روزها برای ثبت یک تراکنش در لجر صبرکنند بلاکچین عملا غیرقابل استفاده خواهد بود.

به تعداد هشی که در هرثانیه توسط تمام ماینرهای شبکه بیت کوین انجام می‌شود hash rate گفته می‌شود.



فاصله زمانی بین تولید بلاک‌ها برحسب دقیقه

تعیین سختی: توافق در عدد هدف

چگونه می‌توان با افزایش تعداد شرکت‌کنندگان در بخت‌آزمایی، پیدا کردن هش معتبر را سخت‌تر و با کاهش تعداد آنها آن را آسان‌تر کرد، تا عرضه بیت کوین و زمان تولید بلاک‌ها ثابت بماند؟

بیت کوین این مسئله را با *تعیین سختی برای ماین کردن*، حل کرده است. از آنجایی که همه افراد شبکه کدهای یکسانی را اجرا می‌کنند که از قوانین مشترکی پیروی می‌کند، و همه افراد یک کپی از تاریخچه تمام بلاک‌ها تا همین زمان را دارند، هرکسی می‌تواند مستقلا سرعت تولید بلاک‌ها را محاسبه کند.

هر زمان که تعداد 2016 بلاک تولید شد، که معمولا باید 2 هفته زمان ببرد، می‌توان بررسی کرد که تولید این تعداد بلاک چقدر زمان برده است و سپس عدد هدف را برای بالا بردن یا کم کردن سرعت تولید بلاک‌ها تنظیم کرد.

همه، 2016 بلاک آخر را دریافت کرده و بر زمان تولید آن تقسیم می‌کنند تا میانگین زمان تولید هر بلاک به‌دست آید. آیا بیشتر از 10 دقیقه است؟ پس سرعت، زیادی کم است. آیا کمتر از ده دقیقه است؟ پس سرعت بالا است.

حالا می‌توان عدد هدف را به گونه‌ای تعیین کرد که متناسب با آنچه که می‌خواهیم، سرعت تولید بلاک‌ها را کم یا زیاد کنیم تا به همان 10 دقیقه فاصله زمانی که در کدها آمده است برسیم.

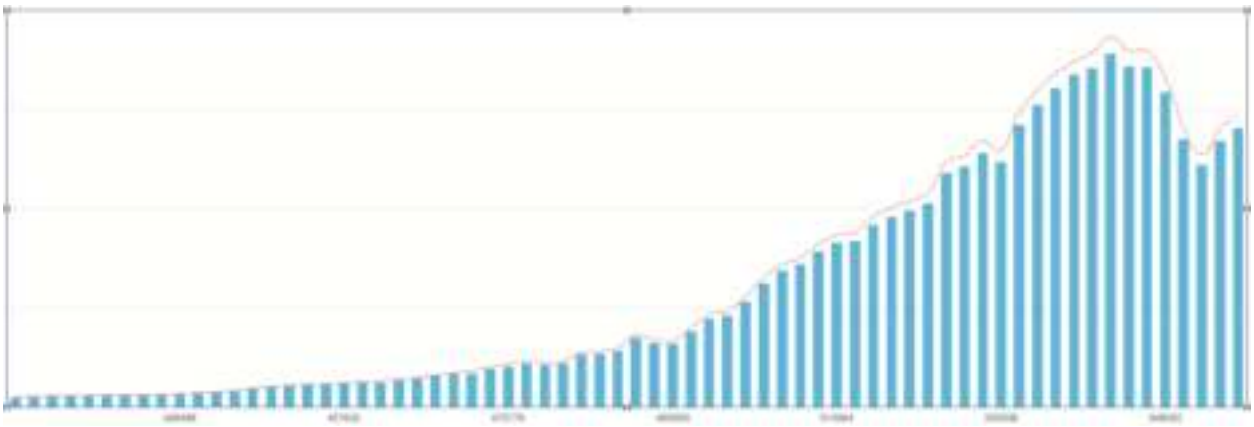
می‌توان عدد هدف را عدد بزرگتری گرفت و بازه هش‌های معتبر را بیشتر کرد که در این صورت ماینرها شانس بیشتری برای برنده شدن خواهند داشت و انرژی کمتری هم مصرف می‌شود، که به آن *کاهش سختی* می‌گویند.

همچنین می‌توان عدد هدف را عدد کوچکی درنظر گرفت که در این صورت بازه هش‌های قابل قبول کوچکتر می‌شود و ماینرها باید انرژی بیشتری برای پیدا کردن هش معتبر هزینه کنند، که به آن *افزایش سختی* گفته می‌شود.

این همچنین به این معناست که برای هر بلاک، براساس تعداد بلاک‌هایی که قبل از آن پیدا شده‌اند (ارتفاع بلاک)، می‌توانیم متوجه شویم که عدد هدف چیست. عدد هدف این اجازه را به ما می‌دهد تا آستانه‌ی برنده شدن یک بلاک خاص (عدد هش تولید شده باید کمتر ازآن باشد) را بدانیم.

این هوشمندانه است- دیگر نیازی به هیچ موجودیت مرکزی وجود ندارد که همه چیز را اطلاع دهد. تمام کاری که باید انجام دهیم این است که خودمان بررسی کنیم عدد هدف چه باشد و اینکه شماره بلیطی که ادعا می‌کند برنده بخت‌آزمایی است کوچکتر از عدد هدف است یا نه.

نمودار زیر هش‌ریت را به صورت خط، و سختی را به صورت میله‌ای نشان می‌دهد. نمودار سختی به شکل پله‌ای است چون با اضافه شدن هر 2016 بلاک، تنظیم می‌شود. می‌توان مشاهده کرد که هر زمان میزان هش‌ریت بالاتر از سختی باشد، میزان سختی افزایش می‌یابد تا هش‌ریت را کاهش دهد. وقتی که هش‌ریت کاهش پیدا می‌کند، همان‌طور که در اکتبر و دسامبر 2018 اتفاق افتاد، از سختی هم کاسته می‌شود. تنظیم سختی شبکه همیشه وابسته به میزان هش‌ریت است.



نمودار 1: مقایسه هش‌ریت و سختی

به دلیل اینکه زمان تنظیم سختی، بعد از تولید هر 2016 بلاک اتفاق می‌افتد، در مدت زمان تولید این بلاک‌ها ممکن است هش‌ریت بالا یا پایین‌تر از چیزی شود که برای عرضه بیتکون درنظر گرفته شده است. درواقع در

حال حاضر سرعت ما در مقایسه با برنامه‌ی عرضه تمام بیت کوین در سال 2140، کمی بیشتر است. افزایش هش‌ریت به معنای تولید تعداد زیادی سخت‌افزار جدید است، با این‌حال تاثیر چندانی روی سرعت تولید بلاک‌ها نخواهد داشت و حتی انتظار می‌رود که در آینده، برابر با آنچه که درنظر گرفته شده است پیش برویم.

تقریبا اختراع بیت کوین را کامل کردیم:

1. جایگزین کردن بانک مرکزی با یک لجر توزیع‌شده
2. ایجاد یک سیستم قرعه‌کشی برای انتخاب اینکه چه کسی در لجر بلاک را ثبت کند
3. وادار کردن شرکت‌کنندگان قرعه‌کشی به هزینه کردن انرژی برای خرید بلیط، با استفاده از هش، و سهولت اعتبارسنجی بلیط برنده برای همه افراد، با کنترل شماره هش تولید شده توسط شرکت‌کنندگان
4. به همه شرکت‌کنندگان در قرعه‌کشی گفته شد که اگر برخلاف قوانین عمل کنند بلاک آنها رد شده و مقدار تراکنش Coinbase به آنها پرداخت نخواهد شد. به این ترتیب یک روش اقتصادی برای جلوگیری از تقلب در شبکه ایجاد و همچنین انگیزه‌ای شد تا همه افراد شبکه از قوانین پیروی کنند.
5. کنترل زمان‌بندی و انتخاب عدد هدف برای قرعه‌کشی با اجازه دادن به همه افراد، که براساس قوانین بیت کوین و با توجه به تاریخچه 2016 بلاک آخر، عدد هدف را برای خود محاسبه و تعیین کنند.
6. کنترل عرضه بیت کوین با استفاده از تعیین سختی که باعث افزایش و کاهش هش‌ریت می‌شود.
7. استفاده از کد متن باز برای اطمینان از اینکه همه می‌توانند صحت اجرای قوانین، اعتبارسنجی تراکنش‌ها، جایزه بلاک و محاسبه سختی را بررسی کنند.

هیچ موجودیت مرکزی وجود ندارد. ما یک سیستم کاملا توزیع‌شده و غیرمتمرکز داریم. هرکسی می‌تواند به آن متصل شود. هرکسی می‌تواند در قرعه‌کشی شرکت کرده و بیت کوین استخراج کند. همه می‌توانند پرداخت کنند. صحت بلاک‌های تولید شده‌ی کل شبکه محرز است و با تراکنش Coinbase به ماینرها جایزه تعلق می‌گیرد، یا با جایزه ندادن تنبیه می‌شوند و ماینرها برای ماین کردن باید انرژی هزینه کنند.

تقریبا تمام مطالب گفته شد، تنها یک مشکل باقی مانده است. زمانی که یک نفر به شبکه متصل می‌شود و یک کپی از لجر درخواست می‌کند، ممکن است کپی‌های متفاوتی از گره‌های مختلف دریافت کند. چگونه یک تاریخچه خطی و واحد ایجاد کنیم و چگونه از بازنویسی مجدد توسط ماینرها جلوگیری کنیم؟

فصل 6: ایمن کردن سکه‌ها

تا اینجا درباره اینکه چطور کپی‌های لجر نگهداری می‌شوند و چطور در یک لجر توزیع‌شده تراکنش‌ها بدون تقلب ثبت می‌شوند، صحبت کردیم. اما اگر برنده قرعه‌کشی بخواهد خرابکاری کند چه؟ آیا فرد برنده می‌تواند تاریخچه بلاک‌ها را در تمام لجرها دستکاری کند؟ آیا Eve,Dave و Farrah می‌توانند با هم تبانی کرده و تاریخچه بلاک‌ها را بازنویسی کنند، و یا موجودی حساب‌ها را تغییر دهند و سکه‌های اضافی به خود بدهند؟

وارد بحث بلاکچین می‌شویم. بلاکچین مفهومی‌ست که در بسیاری از بخش‌های فناوری نفوذ کرده است. بلاکچین چیزی بیشتر از این ایده نیست که بلاک‌های بیت کوین به هم متصل می‌شوند تا مجموعه‌ای از تراکنش‌ها را به مجموعه‌ی بعدی متصل کنند.

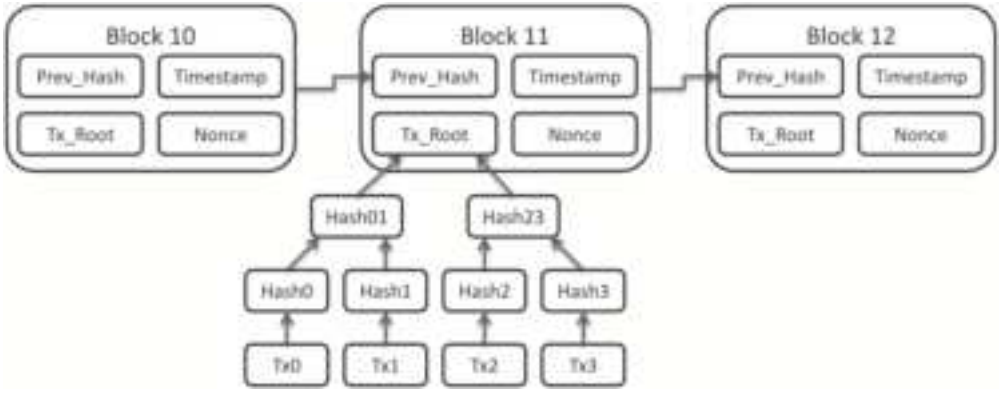
در فصل‌های قبل برای ساده کردن موضوع کمی دروغ گفتیم. زمانی که proof of Work را اجرا می‌کنید، اینطور نیست که فقط تراکنش‌هایی که قرار است در بلاک بعد نوشته شوند و نیز مقدار nonce، هش شوند، بلکه هش بلاک قبلی هم به عنوان ورودی در تابع هش قرار می‌گیرد تا این بلاک را به بلاک قبلی متصل کند.

این کار باعث ایجاد یک تاریخچه برای هر بلاک می‌شود که به اولین بلاک ماین‌شده توسط ساتوشی (Genesis Block) برمی‌گردد. زمانی که یک بلاک در زنجیره نوشته می‌شود باید بررسی شود که تراکنش‌های موجود در آن با توجه به بلاک‌های قبلی تکراری نباشند.

یادآوری می‌کنم که خروجی یک تابع هش، تصادفی است و به تمام داده‌های ورودی وابسته است. پس حالا اصلاح می‌کنم که یک بلاک شامل ورودی‌های زیر است:

1. تراکنش‌هایی که باید در لجر ثبت شوند
2. مقدار تصادفی nonce
3. هش بلاک قبلی که به عنوان تاریخچه لجر خود از آن استفاده می‌کنیم

اگر یکی از این 3 مورد تغییر کند، خروجی هش هم به شکل غیرقابل پیش‌بینی و شدیدی تغییر می‌کند. این کار ویژگی جالبی را ایجاد می‌کند: اگر داده‌های هریک از بلاک‌های قبلی را دستکاری کنید، هش آن تغییر می‌کند، بنابراین هش تمام بلاک‌های بعد از آن هم تغییر خواهد کرد.



نمودار 2: https://upload.wikimedia.org/wikipedia/commons/7/7a/Bitcoin_Block_

هرگونه تغییر در هریک از بلاک‌ها قابل تشخیص است که به این ویژگی Tamper evident گفته می‌شود. اگر کسی تلاش کند یکی از بلاک‌های قدیمی در زنجیره را تغییر دهد، باید مقدار هش بلاک دستکاری شده و همچنین تمام بلاک‌های بعد از آن را نیز مجددا محاسبه کند.

درواقع هر بلاک جدیدی که در شبکه بیت کوین ماین می‌شود، به امنیت بلاک‌های قبلی اضافه می‌کند. یک تراکنش در بلاکی که 6 بلاک تایید شده بعد از آن وجود دارد مثل حک شدن آن روی سنگ است؛ چراکه برای محاسبه 6 بلوک آخر، با توجه به هش‌ریتی که در حال حاضر وجود دارد، مقدار زیادی انرژی باید صرف شود .

مهم است که بدانیم هیچ قانونی برای تعیین نهایی بودن یک تراکنش بیت کوین وجود ندارد. هر پرداخت‌کننده یا فروشنده‌ای خودش تصمیم می‌گیرد که با تصدیق چند بلاک یک تراکنش را نهایی فرض کند. امروزه اکثر افراد 6 بار تایید تراکنش را (تولید 6 بلاک بعد از بلاکی که تراکنش ما در آن است) به عنوان تایید نهایی آن درنظر می‌گیرند ولی به هرتعداد دلخواه قابل تغییر است.

اگر بخواهید یک کتاب دیجیتال که قیمت ناچیزی دارد را بفروشید، ممکن است تنها یک تایید برای شما کافی باشد و یا حتی بدون دریافت هیچ تاییدی به محض اینکه تراکنش در شبکه پخش شد کالای دیجیتال را تحویل دهید. اگر بخواهید یک خانه را بفروشید ممکن است تا 12 بار تایید که تقریبا 2 ساعت طول می کشد، صبر کنید. هرچه بیشتر صبر کنید دفعات بیشتری عملیات proof of work انجام می‌شود و بلاک‌های بیشتری بعد از بلاکی که تراکنش شما در آن قرار دارد ایجاد می‌شوند و هزینه هرگونه تغییر در آن بلاک در دنیای واقعی بیشتر می‌شود.

اگر هش‌ریت بیت کوین به اندازه قابل توجهی کاهش پیدا کند، به این معناست که مقدار انرژی کمتری امنیت بلاک را تضمین می‌کند، پس افراد همیشه می‌توانند تعداد دفعات تایید یک تراکنش را افزایش دهند تا با آسودگی خاطر پرداخت را انجام دهند. اگرچه این فرایند در ابتدا ناامیدکننده به نظر می‌رسد، اما درنظر داشته باشید که تراکنش‌های کارت‌های اعتباری 120 روز بعد از انجام شدن قابل بازگردانی است. از طرف دیگر بیت کوین پولی است که مثل طلا یا پول نقد از شما گرفته نخواهد شد. از این نقطه نظر، برگشت‌ناپذیری و نهایی بودن تراکنش‌های بیت کوین، پیشرفت چشمگیری نسبت به شبکه‌های پرداخت سنتی دارد.

بیایید به مثال فصل 3 برگردیم، جایی که هنری به شبکه متصل شد و کپی‌های متفاوتی از لجر دریافت کرد. لجری که از شارلوت دریافت کرد معتبر بود اما لجر ایو و دیو و فره نادرست بود چون بلاکی که حاوی تراکنش آلیس بود را حذف کرده بودند و می‌توانستند هنری را گول بزنند که آلیس هنوز آن سکه‌ها را دارد. قبل از آنکه بلاک‌ها توسط proof of work به هم متصل شوند، هنری ممکن نبود بتواند حذف بلاک را متوجه شود.

چون هر بلاک دارای proof of work است، او می‌تواند متوجه شود که براساس عدد هدف تقریبا چه مقدار انرژی برای تولید آن صرف شده است.

چون هر بلاک به بلاک قبلی خود اشاره می‌کند، او می‌فهمد که با ایجاد تغییر در تاریخچه یک بلاک نیاز به محاسبه مجدد proof of work نه تنها برای آن بلاک بلکه برای تمامی بلاک‌های بعد از آن نیز هست.

چون تمام تراکنش‌های موجود در یک بلاک را می‌بیند، می‌تواند مطمئن شود که هیچ double spend اتفاق نیفتاده است.

کپشن عکس: برخلاف استخراج طلا که آن هم نیاز به صرف انرژی دارد، فرایند استخراج بیت کوین شبکه را در برابر دستکاری لجر ایمن می‌کند

اگر دونفر همزمان با هم یک بلاک را پیدا کنند چه اتفاقی می‌افتد؟

یک نکته از اجماع سیستم گفته نشده است. تصور کنید که شبکه در سراسر جهان درحال اجرا است. افراد در تمام دنیا از امریکا تا چین به این شبکه سراسری متصل شده‌اند و عملیات proof of work را انجام می‌دهند.

یک نفر در شیکاگو یک بلاک معتبر را پیدا می‌کند. این در شبکه اعلام می‌شود و تمام کامپیوترهای آمریکا این خبر را دریافت می‌کنند. در همین زمان یک‌نفر در شانگهای چین همان بلاک شیکاگو را پیدا می‌کند. گره‌های همسایه هنوز از بلاک آمریکا مطلع نشده‌اند و اول بلاک چین را دریافت می‌کنند.

چون دو بلاک توسط گره‌های همسایه در شبکه پخش شده است حالا دو نسخه از بلاکچین در رقابت با هم داریم. آمریکایی‌ها بلاکچینی را دارند که بلاک آمریکایی در انتهای آن است و چینی‌ها بلاکچینی با بلاک خود را دارند. چون هردو بلاکچین مقدار proof of work یکسانی دارند و هردو حاوی تراکنش‌های معتبر هستند، شبکه به دو بخش تقسیم می‌شود.

به هیچ شخصی نمی‌توان اعتماد کرد که برنده را تشخیص دهد. چه باید کرد؟ برای این مشکل بیت کوین یک راه حل ساده دارد: صبر کنید و ببینید. حالا دو نسخه از بلاکچین وجود دارد که در رقابت با هم هستند. در 10 دقیقه بعدی بلاک دیگری ماین خواهد شد. امریکایی‌ها براساس بلاکچین خود و چینی‌ها نیز براساس بلاکچین خود عملیات ماینینگ را انجام می‌دهند. هرکدام که بتواند بلاک بعدی را ماین کند برنده خواهد شد. چگونه؟ قانونی در کدهای بیت کوین وجود دارد که می‌گوید بلاکچینی که طولانی‌تر است درچنین شرایطی برنده خواهد بود. هرکس انرژی بیشتری را صرف کند برنده است؛ قانونی که ناهمخوانی زنجیره‌ها را براساس طول آنها حل می‌کند و به افتخار ساتوشی ناکاماتو، اجماع ناکاماتو گفته می‌شود.

چینی‌ها بلاک بعدی را ماین می‌کنند. حالا زنجیره آنها یک بلاک بیشتر از آمریکایی‌ها دارد. وقتی آن را در شبکه پخش کنند گره‌های بیت کوین آمریکایی متوجه می‌شوند که گره‌های چینی زنجیره طولانی‌تری را تولید کرده‌اند و بلاکچین خود را اصلاح می‌کنند، یعنی بلاک خود را با دو بلاکی که چینی‌ها ماین کرده‌اند عوض می‌کنند. حالا به بلاکی که امریکایی‌ها ایجاد کرده‌اند orphan یا یتیم می‌گویند؛ چراکه رد شده و ماینر آن جایزه‌ای نگرفته است.

اگرچه من از لفظ امریکایی و چینی برای اشاره به گره‌ها استفاده کرده‌ام، اما در واقعیت گره‌ها چیزی از هویت، موقعیت جغرافیایی و .... یکدیگر نمی‌دانند. تنها چیزی که باید بدانند این است که چه کسی طولانی‌ترین زنجیره از بلاک‌ها را دارد و اینکه تراکنش‌های موجود در زنجیره همگی معتبر هستند (double spend و ... اتفاق نیفتاده).

احتمال تقسیم شدن شبکه به دو زنجیره بسیار کم است. در گذشته یک مورد در ماه و یا کمتر بود اما اخیرا به دلیل ارتقاء تکنولوژی انتشار بلاک و اتصال بین ماینرها در شبکه این اتفاق اصلا رخ نداده است.

یکی از دلایلی که بیت کوین هر 10 دقیقه بلاک‌های نسبتا کوچکی را تولید می‌کند کنترل همین زنجیره‌های orphan است تا کمتر ایجاد شوند. دلیل دیگر، کاهش نیازهای سخت‌افزاری برای اجرای یک گره است تا افراد بیشتری تشویق به اجرای آن در سیستم شوند.

اگر در هرثانیه یک بلاک تولید شود و یا اندازه بلاک خیلی بزرگ باشد، تناقض در بلاک‌های چینی و آمریکایی به احتمال بیشتری اتفاق می‌افتد، چون به لحاظ جغرافیایی فاصله زیادی با هم دارند و مدت زمان بیشتری طول می‌کشد تا به هم دسترسی پیدا کنند. اگر ایجاد orphan ها در شبکه زیاد باشد بلاکچین از بین خواهد رفت چون orphan ها پشت‌سرهم تولید خواهند شد و گره‌ها دیگر قادر به توافق درباره آنها نیستند، درنتیجه تاریخچه خطی تراکنش‌ها از بین خواهد رفت.

یک گره بیت کوین برای جلوگیری از حمله هکرها که ممکن است اطلاعات نادرست ارسال کنند، فقط و فقط نیاز به یک گره صادق که آخرین بلاکچین موجود در شبکه را داشته باشد، دارد. اگر گره شما بخواهد بداند کدام کپی از بلاکچین درست است، کافی‌ست بلاکچینی با دنباله طولانی‌تری از proof of work را پیدا کند. چون دیگران نیز از این قانون پیروی می‌کنند، این اطمینان حاصل می‌شود که درمورد اینکه لجر صحیح کدام است اجماع وجود دارد.

بنابراین برای هکرها کار دشواری است که یک کپی نادرست از بلاکچین را به یک گره بدهند، چون برای رسیدن به هدف خود باید اتصال آن گره به هر گره صادق دیگری را قطع کنند و او را تنها به گره‌های ناسالم متصل سازند.

اگرچه ایجاد انشعاب‌های مختلف از بلاکچین در شبکه بیت کوین عمدتا تصادفی و به دلیل تاخیر انتشار بلاک‌ها است، اما این احتمال نیز وجود دارد که یک موجودیت مخرب بخواهد کنترل بلاک بعدی را دردست بگیرد و از اجماع ناکاماتو سوء استفاده کند. این کار درصورتی ممکن است که فرد مخرب کنترل بیش از 50٪ هش‌ریت را در اختیار بگیرد و طولانی‌ترین بلاکچین را داشته باشد؛ به این مشکل "حمله 51٪" گفته می‌شود و در فصل 9 درباره آن صحبت می‌کنیم.

امنیت و ارزش دلاری بیت کوین

گفته شد که بیت کوین براساس تعداد شرکت‌کنندگان در قرعه‌کشی، که درواقع تعداد ماینرهایی هستند که برای هش‌کردن انرژی صرف می‌کنند، عدد سختی را تعیین می‌کند. اینجا همان نقطه‌ای‌ست که دنیای واقعی، دنیای دیجیتال را لمس می‌کند؛ قیمت بیت کوین، قیمت سخت‌افزار، قیمت انرژی و مقدار عدد سختی که چرخه پیچیده‌ای را ایجاد می‌کند:

1. ماینرها با صرف پول برای انرژی، بیت کوین تولید می‌کنند، چون فکر می‌کنند که بیت کوین ارزشمند است.
2. دلالان، بیت کوین خریداری می‌کنند چون فکر می‌کنند قیمت بیت کوین تا X$ افزایش می‌یابد.
3. ماینرها X$ برای انرژی و سخت‌افزار هزینه می‌کنند تا برای استخراج بیت کوین تلاش کنند.
4. تقاضای بالای خریداران و افزایش قیمت بیت کوین، ماینرهای بیشتری را به سمت استخراج بیت کوین سوق می‌دهد.
5. ماینرهای بیشتر یعنی صرف انرژی بیشتر در شبکه بیت کوین و حتی امنیت بیشتر، که باعث اطمینان بیشتر خریداران از امنیت بیت کوین شده و گاهی اوقات منجر به افزایش قیمت بیت کوین نیز می‌شود.
6. بعد از تولید 2016 بلاک، حضور ماینرهای بیشتر باعث بالا رفتن هش‌ریت می‌شود و این عامل بالا رفتن سختی در شبکه خواهد بود.
7. سختی بالاتر به معنای کوچکتر شدن عدد هدف است- ماینرها بلاک‌های کمتری ماین می‌کنند- که باعث می‌شود ماینرها بیشتر از X$ برای عملیات استخراج بیت کوین هزینه کنند.
8. بعضی از ماینرها هیچ سودی نمی‌کنند، انرژی بیشتری برای ماین کردن صرف می‌کنند و درنتیجه بیت کوین بیشتری برای پرداخت هزینه آن خرج می‌کنند. درین حالت بعضی ماینرها کار را متوقف می‌کنند.
9. 2016 بلاک دیگر تولید می‌شود، سختی شبکه مجددا محاسبه شده و ساده‌تر می‌شود، چون بعضی از ماینرها خاموش شده‌اند.
10. سختی کمتر یعنی ماینرهایی که قبلا سودی نداشته‌اند می‌توانند برگردند و ماین کنند، ویا ماینرهای جدید وارد بازی شوند.
11. برو به مرحله 1.

در یک بازار نزولی، با فروش بیش‌ازحد سکه‌ها از سمت کاربران، این چرخه می‌تواند در جهت دیگری حرکت کند و باعث کاهش قیمت بیت کوین شود (اصطلاحا دامپ اتفاق بیفتد) و ماینرها نتوانند سود کنند. با این وجود، برخلاف آنچه که در رسانه‌ها تحت عنوان "مارپیچ مرگ" درباره آن می‌خوانید، الگوریتم تعیین سختی این اطمینان را حاصل می‌کند که همواره نوعی تعادل بین قیمت بیت کوین و تعداد ماینرها در شبکه وجود خواهد داشت، همچنین ماینرهای ناکارآمد را به نفع ماینرهایی که با کمترین انرژی ممکن کار می‌کنند، کنار می‌زند.

در عمل در این چندسال گذشته، قیمت بیت کوین رشد سریعی داشته است همان‌طور که هش‌ریت افزایش داشته است. هرچه هش‌ریت بالاتر باشد، مورد حمله قرار گرفتن شبکه نیز سخت‌تر خواهد شد، چون برای دردست گرفتن کنترل محتویات بلاک بعدی، به اندازه بیش از نیمی از کل شبکه انرژی و سخت‌افزار نیاز است. امروزه حجم انرژی مصرفی در شبکه بیت کوین تقریبا برابر با انرژی مصرف شده در یک کشور متوسط است.

فصل 7: حساب‌های بدون تعیین هویت

تا اینجا یک لجر توزیع‌شده بدون هیچ مرجع مرکزی، یک سیستم قرعه‌کشی برای انتخاب فردی که در آن بنویسد، و یک سیستم پاداش برای ماینرهای خوب و تنبیه برای بدها، راهی‌ست برای تنظیم سختی ماین کردن در شبکه تا مطمئن شویم برنامه عرضه بیت کوین ثابت است و یک سیستم برای بررسی اعتبار زنجیره ایجاد کرده‌ایم.

اکنون بیایید درباره هویت صحبت کنیم. در یک سیستم بانکی سنتی، شما با معرفی خود به بانک پول جابه‌جا می‌کنید، از طریق ارایه شناسه به صورت حضوری، یا ارایه نام کاربری و پسورد در برنامه هاب بانک. بانک مطمئن است که هیچ دو نفری دارای یک شناسه نیستند.

حال که هیچ مرجعی برای پیگیری هویت افراد نداریم، چطور می‌توانیم در سیستم مالی بیت کوینی یک حساب جدید باز کنیم، و چطور می‌توان مطمئن شد وقتی آلیس می‌خواهد به باب پرداخت کند واقعا این آلیس است و اجازه جابه‌جا کردن پول را دارد؟

ایجاد یک "حساب بیت کوین"

از آنجا که نمی‌توانیم به یک واسطه مرکزی مثل بانک، برای ثبت تمامی حساب‌ها اطمینان کنیم و چون افراد بدون اجازه می‌توانند بیایند و بروند، حساب‌ها چگونه مدیریت می‌شوند؟

چه می‌شود اگر هرکس نام کاربری و پسورد خودش را ثبت کند؟ یک بانک معمولا بررسی می‌کند که این نام کاربری قبلا استفاده نشده باشد، اما این روش اینجا ممکن نیست، چون هیچ مرجعی وجود ندارد که تمام شناسه‌ها را داشته باشد. پس به چیزی قوی‌تر و بزرگتر و خاص‌تری از یک نام کاربری و کلمه عبور نیاز داریم. این تکنیک با توجه به فصل‌های قبلی باید آشنا باشد. دوباره نیاز به یک عدد بزرگ تصادفی داریم.

همان‌طور که خرید بلیط بخت‌آزمایی با تولید شماره‌های تصادفی ممکن شد، از همین روش برای ایجاد حساب‌ها نیز استفاده می‌کنیم. برای ایجاد یک "حساب بیت کوین" که به آن آدرس می‌گویند، ابتدا یک جفت عدد 256 بیتی تولید می‌کنیم که از لحاظ ریاضی با هم مرتبط هستند، به نام public/private key (کلیدهای عمومی و خصوصی). دوباره به اندازه 2^{256} جفت کلید امکان تولید دارند، به اندازه اتم‌های جهان. بنابراین احتمال اینکه دو نفر جفت کلیدهای مشابهی را تولید کنند غیرممکن است.

این جفت کلید ویژگی‌های جالبی دارد. می‌توان از آن، هم برای رمزنگاری و هم برای رمزگشایی یک پیغام استفاده کرد. علاوه‌براین شما می‌توانید کلید عمومی خود را در سراسر جهان به اشتراک بگذارید. با دانستن کلید عمومی کسی نمی‌تواند به کلید خصوصی شما دسترسی پیدا کند.

بیایید ببینیم آلیس چطور برای باب سکه ارسال می‌کند. برای دریافت یک تراکنش، باب جفت کلید عمومی و خصوصی را تولید می‌کند و کلید خصوصی را کاملا محرمانه نگه می‌دارد. او یک آدرس ایجاد کرده است، یک عدد بزرگ براساس کلید عمومی. سپس باب این شماره آدرس را با آلیس به اشتراک می‌گذارد، حالا آلیس می‌تواند برای باب سکه ارسال کند.

آلیس باید به شبکه اطلاع دهد که می‌خواهد از آدرس عمومی خودش به آدرس عمومی باب سکه بفرستد. اما چطور ثابت کند که اجازه‌ی خرج کردن از این آدرس را دارد؟ آلیس این کار را با اثبات اینکه کلید خصوصی خود متعلق به این آدرس است، انجام می‌دهد، بدون اینکه کلید خصوصی خود را افشا کند.

امضای دیجیتال چیزی است که این اثبات را انجام می‌دهد. آلیس یک تراکنش ایجاد می‌کند، که در اصل یک دیتا است چیزی شبیه به "آدرس 12345 مقدار 2 بیت کوین برای آدرس 5678 ارسال می‌کند" با این تفاوت که شماره آدرس یک عدد بزرگ است. سپس آلیس تراکنش خود را هش کرده و با کلید خصوصی خود هش را رمزنگاری و یک امضای دیجیتال ایجاد می‌کند.

وقتی آلیس تراکنش خود را در شبکه منتشر کرد، کلید عمومی خود را هم اعلام می‌کند (که از کجا ارسال می‌کند). چون همه کلید عمومی آلیس را دارند می‌توانند امضای دیجیتال را رمزگشایی کنند. اما آنها تنها درصورتی قادر به رمزگشایی خواهند بود که تراکنش واقعا با کلید خصوصی که فقط آلیس آن را می‌داند، رمزنگاری شده باشد.

تنها مزیتی که رمزگشایی امضای دیجیتال دارد این است که به همه اجازه می‌دهد تا بدانند آلیس کلید خصوصی این آدرس را دارد، بدون اینکه نیازی به افشای کلید خصوصی باشد.

وقتی پولی را در بانک جابه‌جا می‌کنید، شناسه کاربری و رمزعبور خود را به بانک می‌دهید. وقتی چکی را می‌نویسید، آن را امضا می‌زنید تا تصدیق کنید این چک را خودتان نوشته‌اید. وقتی بیت کوین جابه‌جا می‌کنید ثابت می‌شود که مالک کلید آدرس بیت کوین هستید.

برخلاف امضای روی چک بانکی یا رمز بانکی شما، امضای دیجیتال شما مختص داده‌های یک تراکنش یکتا است. از این جهت نمی‌توانند دزدیده و یا در تراکنش دیگری استفاده شوند. هر تراکنش امضای متفاوتی دارد حتی اگر براساس کلید خصوصی یکسانی باشد.

آیا می‌توان یک کلید خصوصی را حدس زد؟

بیایید احتمال حدس زدن یک کلید خصوصی، که به شما امکان انتقال سکه‌ها از آدرس عمومی متعلق به آن را می‌دهد، بررسی کنیم. یادآوری می‌کنم که یک کلید از حداکثر 256 بیت ساخته می‌شود. هر بیت تنها دو مقدار می‌تواند بگیرد (صفر و یک). هر بیت را مثل بازی شیر یا خط می‌توانید تصور کنید.

بررسی مختصری از احتمالات پایه‌ای: احتمال وقوع چند رویداد با ضرب کردن احتمال رخ دادن تک‌تک رویدادها محاسبه می‌شود. اگر در پرتاب سکه احتمال شیر آمدن 1/2 باشد، بنابراین احتمال شیر آمدن در دوبار پرتاب سکه برابر با 1/4 یا یک به 4 خواهد بود. اگر 2 بیت داشته باشیم، مثل دوبار پرتاب سکه است. $2^2=4$، بنابراین شانس شما 1 به 4 است.

نتیجه پرتاب 8 بار پشت سر هم سکه، 2^8 است یا 1 به 256.

یک پلاک دارای 6 رقم یا حرف است. تعداد حروف الفبای انگلیسی 26 و تعداد 10 رقم وجود دارد، بنابراین جمعا 36 کاراکتر برای پلاک وجود دارد. چون پلاک 6 رقمی است تعداد پلاک‌هایی که می‌توان ایجاد کرد 36^6 خواهد بود. پس احتمال حدس زدن پلاک یک در 2,176,782,336 است.

یک کارت اعتباری 16 رقم دارد. هر رقم می‌تواند 10 مقدار داشته باشد. پس احتمال حدس زدن شماره کارت اعتباری 10^{16} است، یعنی یک بر 10,000,000,000,000,000 .

در زمین حدود 10^{50} اتم وجود دارد. اگر به طور تصادفی یکی از اتم‌ها را درنظر بگیریم، شانس شما در حدس زدن آن چیزی حدود

1 بر 1,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000

خواهد بود.

یک کلید خصوصی 256 بیت دارد، یعنی 2^{256} یا حدود 10^{77}. درواقع عددی به بزرگی حدس زدن یک اتم خاص از کل هستی و یا 9 بار متوالی برنده شدن در بخت‌آزمایی: یک شانس در

115,792,089,237,316,195,423,570,985,
008,687,907,853,269,984,665,640,564,039,457,584,
007,913,129,639,936

اما اگر یک کامپیوتر بسیار قدرتمند برای حدس زدن داشته باشید چه؟ پرداختن به این موضوع بیش از این در اینجا جایز نیست. در پست‌های Reddit[1] می‌توانید درباره این موضوع بخوانید. با وجود اینکه متن تخصصی است اما پاراگراف آخر آن می‌تواند تصور خوبی از لیست کردن تمام 256 بیت ممکن را به شما بدهد:

"اگر بتوانید تمام سیارات را به عنوان حافظه استفاده کنید، یک بایت برای هر اتم ذخیره کنید، از ستاره‌ها به عنوان سوخت استفاده کنید، و یک تریلیون کلید در ثانیه بازیابی کنید، نیاز به 37 اکتیلیون زمین برای ذخیره آن و 237 خورشید برای تامین انرژی سخت‌افزارها نیاز دارید و تمام این فرایند 3.6717 octodecillion سال طول می‌کشد."

اساسا حدس زدن کلید خصوصی شخص دیگر غیرممکن است. نه فقط این، بلکه تعداد آدرس‌های بیت کوین به قدری زیاد است که بهتر است برای هر تراکنشی که ایجاد می‌شود یک آدرس جدید ساخت. بنابراین به‌جای داشتن یک حساب بانکی، شما می‌توانید هزاران یا حتی میلیون‌ها حساب بیت کوین داشته باشید؛ برای هر تراکنشی که دارید، یک حساب.

[1] تمام پست‌های Reddit درباره حدس زدن 256 بیت در لینک زیر موجود است:
https://bit.ly/2Dbw9Qd

ممکن است ناامیدکننده باشد که امنیت حساب بیت کوین شما براساس شانس تامین می‌شود، اما امیدوارم که نوشته بالا این اطمینان را ایجاد کند که امنیت این حساب بسیار بیشتر از رمزعبور حساب بانکی شماست که در یک سرور مرکزی ذخیره شده و برای هکرها قابل دسترس است.

بررسی موجودی حساب

حالا زمان تصحیح آخرین دروغ سفیدی است که درباه نحوه کار بیت کوین گفتم. مانده حساب‌ها در لجر ثبت نمی‌شود، به‌جای آن بیت کوین از یک مدل به نام UTXO استفاده می‌کند: Unspent Transaction Output

ایده UTXO به این صورت است که، هر تراکنشی مجموعه‌ای از ورودی‌ها دارد که برای تولید خروجی‌های جدید استفاده می‌شوند. مثل این است که تعدادی سکه را به یک دستگاه بدهیم تا آنها را ذوب کند و سکه‌های جدید از هر نوعی که بخواهیم را ضرب کرده و به ما بدهد. به بیان ساده UTXO خروجی یک تراکنش است- یک سکه با توجه به تراکنش‌های قبلی، که شامل تراکنش Coinbase برای جایزه بلاک است، ساخته می‌شود- که هنوز به آدرس دیگری پرداخت نشده است.

به عنوان مثال، آلیس دارای یک آدرس است که 1 بیت کوین دارد. او می‌خواهد 0.3 بیت کوین برای باب ارسال کند. او یک تراکنش ایجاد می‌کند با 1 بیت کوین UTXO به عنوان ورودی و دو خروجی. یک UTXO جدید به ارزش 0.3 به عنوان خروجی به آدرس باب دارد و یک UTXO جدید دیگر به ارزش 0.7 به عنوان خروجی برای بازگرداندن به آدرس آلیس. تغییر ایجادشده می‌تواند به همان آدرسی برگردد که آلیس ارسال را از آن انجام داده و یا آلیس می‌تواند برای امنیت بیشتر آدرس جدیدی را ایجاد و از آن استفاده کند.

از آنجایی که در زنجیره بلاک‌ها راهی وجود ندارد که تشخیص دهیم هر آدرس متعلق به چه کسی است (برای این منظور باید کلیدهای خصوصی هر آدرس را بدانید و آنها را به دنیای واقعی گره بزنید)، مدل UTXO با فراهم آوردن این امکان که در هر جابه‌جاییِ سکه‌ها آدرس‌های جدید ساخته شود، مکانیزم بسیار خوبی برای ایجاد حریم خصوصی به وجود آورده است.

بنابراین برای کنترل موجودی حساب یک آدرس خاص، درواقع باید تمام UTXO هایی را که این آدرس به عنوان خروجی دارد را جمع‌آوری کنیم. مجموع کل UTXO ها در بیت کوین وقتی افراد از یک آدرس به آدرس‌های مختلف پرداخت انجام می‌دهند، رشد می‌کند، و وقتی افراد تراکنش‌های "ادغامی" را ایجاد می‌کنند که از آدرس‌های مختلف پرداخت به یک آدرس انجام می‌شود، کاهش پیدا می‌کند.

مدل UTXO تشخیص Double Spend را هم بسیار ساده می‌کند، چون هر UTXO خاص تنها می‌تواند به یک نفر ارسال شود و نیازی به دانستن تمام تاریخچه پرداخت‌های انجام شده از یک حساب خاص نیست.

همچنین می‌توان در یک زمان تعداد زیادی UTXO ایجاد کرد و از بین برد، می‌توان تراکنش‌های پیچیده‌ای که ورودی و خروجی‌های مختلفی را با هم ترکیب می‌کنند ایجاد کرد. این ویژگی ایده "ترکیب سکه‌ها" را می‌دهد که در آن چندین نفر می‌توانند در یک تراکنش بیت کوین، که هرتعدادی از ورودی‌ها را برای تولید هرتعداد خروجی ترکیب می‌کند، شرکت کنند، و از این طریق تاریخچه UTX ها پنهان می‌ماند.

به علاوه این اجازه را به افراد می‌دهد که به صورت تلفیقی سکه‌ها را از آدرس‌های مختلف به یک آدرس ادغام کنند ویا سکه‌ها را بین آدرس‌های مختلف پخش کنند تا امنیت و حریم خصوصی افزایش پیدا کند.

کیف پول

ایجاد یک حساب، چیزی بیشتر از ساخت یک عدد تصادفی 256 بیتی به عنوان کلید خصوصی نیست، و ما می‌توانیم هزاران و یا حتی میلیون‌ها حساب ایجاد کنیم. به همین دلیل نیاز به مکانیزمی داریم تا همه این حساب‌ها را پیگیری کنیم. در بیت کوین واژه کیف پول به هرنوع وسیله‌ای که با آن بتوانیم کلیدهای خود را مدیریت کنیم، اشاره می‌کند. این وسیله می‌تواند به سادگیِ یک تکه کاغذ باشد و یا به پیچیدگی یک سخت‌افزار.

نرم‌افزار اصلی بیت کوین که توسط ساتوشی ارائه شد به همراه خود یک نرم‌افزار کیف پول داشت. این کیف پول جفت کلیدهای عمومی و خصوصی را می‌تواند ایجاد کند. (یادآوری می‌کنم که کلید عمومی برای ساختن آدرس بیت کوین استفاده می‌شود و کلید خصوصی برای امضا کردن تراکنش‌های پرداخت از آن آدرس)

برخلاف کیف پول بانکی که معمولا در قالب یک اپلیکیشن تحت وب یا موبایل است، بیت کوین کاملا یک سیستم باز است. به همین دلیل صدها کیف پول مختلف وجود دارد که بیشتر آنها رایگان هستند، بسیاری متن باز و همچنین نیمی از آنها کیف پول‌های سخت‌افزاری هستند با مزایای بیشتر. هرکسی با دانش برنامه‌نویسی کامپیوتر می‌تواند کیف پول خود را بسازد یا سورس کد کیف پول‌ها را بخواند تا مطمئن شود هیچ تقلبی درکار نیست. این مزیت دیگری در بیت کوین است که برخلاف نرم‌افزارهای بانکی، ایده عدم نیاز به‌خوبی استفاده می‌شود.

کلید خصوصی تنها چیزی است که برای خرج کردن سکه‌های‌تان نیاز دارید، پس باید به خوبی از آن مراقبت کنید. اگر کسی کارت اعتباری شما را سرقت کند، می‌توانید با کمپانی تماس گرفته و با تنظیم شکایت پول خود

را پس بگیرید. در بیت کوین، چنین واسطه‌ای وجود ندارد. اگر کسی کلید خصوصی شما را در اختیار داشته باشد می‌تواند سکه‌های شما را کنترل کند و هیچ‌کسی نیست که شما بتوانید با او تماس بگیرید و مشکل را حل کنید.

همچنین کلیدهای خصوصی، بسیار مستعد گم‌شدن هستند. اگر کیف پول خود را در کامپیوتر ذخیره کنید و کامپیوتر دزدیده شود و یا آتش بگیرد، مشکل خواهید داشت. اگر پس از هربار دریافت پول، با بهترین روش‌های بیت کوین آدرس جدید می‌سازید و بعد از آن کلیدهای خصوصی را ذخیره و از آن پشتیبان تهیه می‌کنید، این کار به‌سرعت باعث سنگین شدن سیستم شما می‌شود.

درطول زمان، بیت کوین راه‌حل‌هایی برای این مشکل ارائه داده است. در سال 2012، BIP32 (Bincoin Improvement Proposal، که در آن افراد می‌توانند ایده خود را برای ارتقاء بیت کوین به اشتراک بگذارند) پیشنهاد ساخت کیف پول‌های سلسله مراتبی قطعی که به آن HD می‌گویند را مطرح کرد. ایده پشت این پیشنهاد استفاده از تنها یک عدد تصادفی (seed) است که با آن می‌توان تمام زنجیره جفت کلیدهای عمومی و خصوصی را ایجاد کرد: آدرس‌های بیت کوین و امضای آنها.

امروزه هر نرم‌افزار یا سخت‌افزار کیف پولی که دردسترس است، به صورت اتوماتیک کلیدهای جدیدی برای هر تراکنش شما ایجاد می‌کند و شما فقط لازم است تنها یک seed را ذخیره کنید.

در سال 2013، BIP39 ذخیره کلیدها را حتی آسان‌تر کرد. به‌جای استفاده از اعداد کاملا تصادفی، کلیدها می‌توانند در قالب کلمات قابل فهم برای انسان تولید شوند. به عنوان مثال:

```
witch collapse practice feed shame open despair creek road again
ice least
```

با این روش ذخیره کلیدها بسیار آسان است: می‌توانید این seed را روی تکه‌ای کاغذ بنویسید و در محل امنی نگهداری کنید. حتی می‌توانید عبارت‌ها را به‌خاطر بسپارید و ثروت خود را در حافظه‌تان حمل کنید.
علاوه بر این یک آدرس بیت کوین ممکن است بیش از یک کلید خصوصی برای دسترسی به آن داشته باشد. آدرس‌های چند-امضایی یا multisig می‌توانند انواع مختلفی از طرح‌های امنیتی را به کار گیرند. به عنوان مثال افراد می‌توانند حساب‌های مشترک داشته باشند که 1-از-2 باشد، یعنی هریک از آنها می‌تواند تراکنش‌ها را امضا کند و یا ممکن است 2-از-2 باشد که در این صورت به کلیدهای هردو طرف برای پرداخت نیاز خواهد بود.
می‌توان با استفاده از مدل چند امضایی 2-از-3 یک سیستم Escrow (ضمانتی) ایجاد کرد. خریدار یک کلید خواهد داشت، فروشنده یک کلید و کلید سوم به یک داور اختصاص دارد. اگر خریدار و فروشنده هردو توافق

داشته باشند می‌توانند تراکنش را امضا کنند، ولی اگر اختلاف نظر وجود داشته باشد داور می‌تواند با یکی از طرفین توافق کند تا تراکنش را امضا کنند.

می‌توان مدل 3-از- 5 را برای محافظت از کلیدها استفاده کرد، به این طریق که حتی اگر 2 کلید از 5 کلید را از دست بدهید، باز هم قادر به استفاده از حساب خود خواهید بود. می‌توان 2 تا از کلیدها را در جای دیگری ذخیره کرد، 2 تا را نزد دو دوست قابل اطمینان که یکدیگر را نمی‌شناسند و یکی را نزد سرویس‌های خاصی، مثل BitGo که می‌توانند مشترکا تراکنش‌های شما را امضا کنند، ذخیره کنید. با این کار درحالی‌که از کلیدهای خود محافظت می‌کنید، سرقت بیت کوین‌های شما بسیار سخت خواهد شد.

حتی می‌توان از این هم فراتر رفت و آدرس‌هایی را ساخت که دسترسی به آنها شرایط پیچیده‌تری داشته باشد، مثل اعداد پنهان یا قفل کردن برای یک بازه زمانی خاص. مثلا می‌توانید یک آدرس بیت کوین بسازید که به مدت 10 سال نتوانید از آن خرج کنید؛ هیچ‌کس نمی‌تواند شما را مجبور به تغییر آن کند. این، تغییر زندگی و تغییر جهان است. پیش از این هرگز امکان نداشت بتوان دارایی خود را چنین ایمن از سرقت حمل کرد.

فصل 8: نرم‌افزار Bitcoin client

تا اینجا یک سیستم توزیع‌شده کاربردی برای نگهداری و پیگیری و انتقال پول ایجاد کردیم. بیایید آنچه را که ایجاد کرده‌ایم مرور کنیم:

1. یک لجر توزیع‌شده، یک کپی از آن در اختیار همه اعضا قرار دارد.
2. یک سیستم قرعه‌کشی براساس proof of work و تنظیمات سختی برای حفظ ایمنی و ثابت نگه داشتن حجم عرضه بیت کوین.
3. یک سیستم اجماع که این اطمینان را می‌دهد که همه اعضا می‌توانند تمام تاریخچه بلاکچین را برای خود ارزیابی کنند، با استفاده از یک نرم‌افزار متن باز به نام Bitcoin Client.
4. یک سیستم شناسایی که از امضای دیجیتال برای دریافت بیت کوین بدون نیاز به یک مرجع مرکزی استفاده می‌کند.

حال زمان آن است که یکی از جالب‌ترین و مهمترین چیزها را درمورد بیت کوین حل کنیم: قوانین از کجا می‌آیند و چگونه اجرا می‌شوند؟

نرم‌افزار بیت کوین

باتوجه به فصل‌های قبل، فرض می‌کنیم که همه در شبکه از یک قانون پیروی می‌کنند: double Spend را رد می‌کنند، اطمینان حاصل می‌کنند که هر بلاک مقدار proof of work درستی دارد، هر بلاک به بلاک قبل از خود در راس بلاکچین اشاره می‌کند، و تمام چیزهای دیگری که افراد درطول زمان درباره آنها توافق کرده‌اند.

گفته شد که بیت کوین یک نرم‌افزار متن باز است. متن باز یعنی هرکسی می‌تواند کدهای آن را بخواند، و همچنین هرجایی از کد را که بخواهد برای خود تغییر دهد. چگونه؟

بیت کوین یک *پروتکل* است. در نرم‌افزار کامپیوتر، این واژه به معنای مجموعه‌ای از قوانین است که نرم‌افزار از آنها پیروی می‌کند. بااین‌حال، تا زمانی‌که شما مجموعه قوانینی که همه از آن پیروی می‌کنند را اجرا کنید، می‌توانید نرم‌افزار خود را ویرایش کنید. وقتی گفته می‌شود که کسی "گره بیت کوین را اجرا می‌کند"، درواقع به معنای اجرا کردن نرم‌افزار بیت کوین است که از پروتکل‌های بیت کوین صحبت می‌کند.

این نرم‌افزار می‌تواند با سایر گره‌های بیت کوین ارتباط برقرار کند، تراکنش‌ها و بلاک‌ها را به آنها انتقال دهد، گره‌های دیگر را پیدا کند تا با آنها جفت شود و چیزهای دیگر.

جزئیات واقعیِ نحوه اجرای نرم‌افزار در افراد مختلفی که آن را اجرا می‌کنند متفاوت است. درواقع روش‌های زیادی برای پیاده‌سازی پروتکل بیت کوین وجود دارد. شناخته‌شده‌ترین آنها Bitcoin Core است که نسخه توسعه‌یافته‌ی نرم‌افزاری است که برای اولین بار توسط ساتوشی ناکاماتو منتشر شد.

کلاینت‌های دیگری نیز وجود دارند؛ بعضی از آنها حتی به زبان‌های دیگری نوشته شده‌اند و توسط افراد مختلفی نگهداری می‌شوند. چون اجماع در بیت کوین بسیار مهم است (یعنی تمام گره‌ها باید بر سر اینکه بلاک‌ها معتبر هستند یا نه توافق داشته باشند) اکثریت گره‌ها نرم‌افزار مشابهی (Bitcoin core) را اجرا می‌کنند تا از اشکالاتی که ممکن است باعث اختلاف‌نظر گره‌ها درمورد اعتبار بلاک شود، جلوگیری کنند.

چه کسی قوانین را تعیین می‌کند؟

قوانینی که بیت کوین را ایجاد کرده‌اند در Bitcoin Core نوشته شده‌اند، اما چه کسی درمورد قوانین تصمیم می‌گیرد؟ چرا می‌گوییم بیت کوین اندک است درحالی‌که ممکن است یک نفر نرم‌افزار را ویرایش کند و تعداد بیت کوین را از 21 میلیون به 42 میلیون تغییر دهد؟

چون سیستم توزیع‌شده است، تمامی گره‌ها در سیستم باید درمورد قوانین توافق داشته باشند. اگر شما ماینری باشید که تصمیم گرفته نرم‌افزار را به‌گونه‌ای تغییر دهد که دوبرابر آنچه که در تنظیمات بیت کوین آمده، جایزه دریافت کند، وقتی بلاکی را ماین کنید بقیه گره‌ها بلاک را رد خواهند کرد. تغییر قوانین بسیار سخت است چون هزاران گره توزیع‌شده در سراسر جهان هستند که قوانین را اجرا می‌کنند.

مدل حاکمیت بیت کوین به راحتی قابل فهم نیست، به‌خصوص برای کسانی مثل ما که در یک دموکراسی غربی زندگی می‌کنند. ما عادت کرده‌ایم که با رای دادن حکومت کنیم، رای دادن یعنی اکثریت مردم می‌توانند تصمیم بگیرند که کاری انجام شود، قانونی تصویب شود و آنچه که می‌خواهند را به اقلیت مردم تحمیل کنند. اما حاکمیت بیت کوین بیشتر شبیه به آنارشی است تا دموکراسی. بیایید نگاهی به نحوه کنترل این مسئله در سیستم بیندازیم:

گره‌ها: هر عضو در شبکه بیت کوین یک گره را اجرا می‌کند و حق انتخاب دارد که کدام نرم‌افزار آن را اجرا کند. اگر نرم‌افزار مخرب باشد و سعی بر انجام کاری شبیه به افزایش جایزه را داشته باشد، طبعا هیچ‌کس آن را اجرا نخواهد کرد. گره، یعنی هرکسی که بیت کوین را پذیرفته است، مانند بازرگانان، صرافی‌ها، ارائه‌دهندگان کیف پول و افرادی که به صورت روزمره از بیت کوین استفاده می‌کنند.

Miner ها: بعضی از گره‌ها ماین می‌کنند، یعنی برق مصرف می‌کنند تا اجازه نوشتن در لجر بیت کوین را داشته باشند. این کار امنیت شبکه بیت کوین را تامین می‌کند؛ چراکه هزینه دستکاری در لجر بسیار زیاد است. چون ماینرها تنها کسانی هستند که در لجر می‌نویسند، ممکن است فکر کنید که آنها هستند که قوانین را تعیین می‌کنند، اما اینطور نیست. آنها فقط قوانینی که توسط گره‌های بیت کوین تنظیم شده است را اجرا می‌کنند. اگر ماینرها شروع به تولید بلاک‌هایی کنند که جایزه اضافی دارند، گره‌های دیگر آنها را رد می‌کنند، چون باعث بی‌ارزش شدن سکه‌ها می‌شود. پس هر کاربری که یک گره را اجرا می‌کند عضوی از حکومت آنارشیستی است- آنها تعیین می‌کنند که چه قوانینی باید وجود داشته باشد و هرگونه نقض این قوانین را رد می‌کنند.

کاربران/سپرده‌گذاران: کاربران افرادی هستند که مثل گره‌ها بیت کوین خریدوفروش می‌کنند. بسیاری از کاربران گرهی را اجرا نمی‌کنند اما به گرهی که توسط ایجادکننده کیف پول‌شان اجرا می‌شود اعتماد می‌کنند، چون ارائه‌دهندگان کیف پول مثل پراکسی، طبق خواسته و میل کاربر عمل می‌کنند. کاربران هستند که ارزش سکه‌ها در بازار آزاد را تعیین می‌کنند. حتی اگر ماینرها و بیشتر گره‌های در سیستم بخواهند با هم تبانی کنند و تغییراتی مثل افزایش نرخ جایزه را در سیستم ایجاد کنند، کاربران می‌توانند ارز را دامپ کنند، قیمت آن را پایین

بیاورند و شرکت‌های متخلف را کنار بزنند. یک گروه متعصب از کاربران همیشه می‌توانند نسخه بیت کوین خود را فعال نگه دارند، حتی اگر بیت کوین تبدیل به چیزی شود که دیگران دوست نداشته باشند.

توسعه‌دهندگان: Bitcoin Core بزرگترین نرم‌افزار bitcoin client است که صدها نفر از بهترین توسعه‌دهندگان و شرکت‌های رمزارزی را به خود جلب کرده است. هسته اصلی پروژه بسیار امن است چراکه این نرم‌افزار شبکه‌ای را ایجاد کرده است که امروزه امنیت صدها میلیون دلار را تامین می‌کند. هر تغییری که پیشنهاد شود به دقت مورد بررسی قرار می‌گیرد. فرایند بررسی کدها و پیشنهادها کاملا باز است و هرکسی می‌تواند به آن ملحق شود، اظهار نظر کند و یا کد ارائه دهد. اگر توسعه‌دهندگان تخلف کنند و چیزی را معرفی کنند که هیچ‌کس تمایل به اجرای آن ندارد، کاربران به سادگی نرم‌افزار دیگری را اجرا خواهند کرد (شاید نسخه قدیمی‌تر را اجرا کنند و یا شروع به توسعه چیز جدیدی کنند). به همین دلیل توسعه‌دهندگان باید تغییراتی را ایجاد کنند که مطابق با خواست کاربران باشد در غیر این صورت جایگاهشان را از دست خواهند داد.

اکوسیستم بیت کوین درواقع رقص ظریفی بین صدها و هزاران عضو آن است، که اگرچه همه آنها خودخواهانه عمل می‌کنند و معمولا در رقابت با یکدیگر هستند، اما یک سیستم بسیار انعطاف‌پذیر و عالی را ایجاد کرده‌اند. بیت کوین به راستی یک سیستم آزاد است که شخص خاصی مسئول آن نیست.

فصل9: گذشته، حال و آینده

حالا که شبکه بیت کوین را کاملا یاد گرفتیم می‌توانیم چند رفتار جالب که درطول ده سال گذشته در سیستم شکل گرفته است را بررسی کنیم.

ASIC ها و استخرهای ماینینگ

در ابتدا ساتوشی اولین بیت کوین را با استفاده از CPU کامپیوتر ماین کرد. چون سختی اولیه سیستم بسیار کم بود، تولید این سکه برای کامپیوتر او تقریبا گران درآمد.

به مرور زمان، با دستکاری نرم‌افزار، عملیات ماینینگ بهتر و بهتر شد. درنهایت از پردازنده خاصی به نام GPU استفاده شد که روی کارت‌های گرافیک وجود داشت و برای بازی استفاده می‌شد.

با استفاده از GPU عملیات ماینینگ هزاران بار بهتر از CPU انجام شد. در این زمان افرادی که از CPU استفاده می‌کردند کسر کمتری از هش‌ریت را نسبت به ماینرهای GPU دردست داشتند که با افزایش سختی، ماین کردن کاملا برای آنها بدون سود بود.

با تولید ASIC (Application Specific Integrated Circuit) میزان بهره‌وری ماینینگ افزایش پیدا کرد. ASIC ها چیپ‌های سخت‌افزاری هستند که تنها یک کار انجام می‌دهند؛ تابع Sha256 بیت کوین را اجرا می‌کنند نه چیزی بیشتر. ASIC تنها مختص اجرای این الگوریتم خاص است که باعث شد برای ماین کردن، هزاران بار به‌صرفه‌تر از GPU باشد و آنها را غیرقابل استفاده کرد، درست همان کاری که GPU با CPU انجام داد. هر چندسال یک بار نسل جدیدی از ASIC عرضه می‌شود که با توجه به پیشرفت چشمگیری که در راندمان دارد نسخه‌های قبل خود را از رده خارج می‌کند.

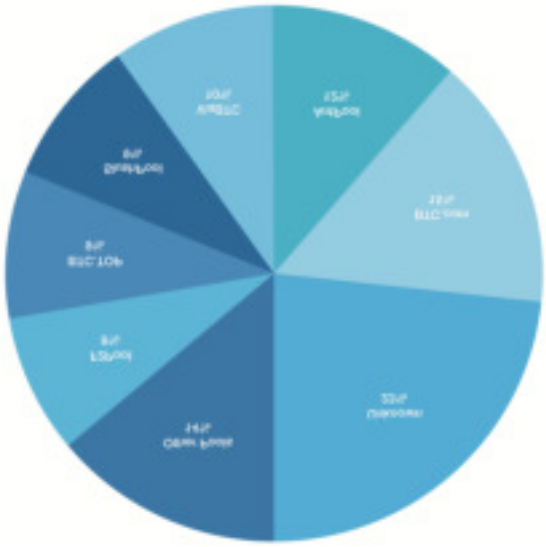
ماینرهای اولیه در شبکه، برای تولید بیت کوین برق کمتری مصرف می‌کردند. با افزایش قیمت بیت کوین، ماینرهای زیادی به شبکه پیوستند و درنتیجه سختی بالا رفت و تولید بیت کوین گران و گران‌تر شد.

یک مسئله در استخراج بیت کوین این است که قطعیت ندارد، مثل پرتاب تاس. یعنی شما ممکن است صدها دلار برای مصرف برق هزینه کنید و هیچ بلاک معتبری هم پیدا نکنید.

در سال 2010 چیز تازه‌ای به نام استخر ماینینگ (mining pool) ایجاد شد تا مشکل ماینرهایی را که انرژی مصرف می‌کنند اما جایزه‌ای دریافت نمی‌کنند را حل کند. mining pool چیزی شبیه به بیمه‌های درمانی است و ریسک کار را به اشتراک می‌گذارد.

همه ماینرها عملیات ماین یا استخراج را برای استخر انجام می‌دهند، بنابراین یک ماینر بسیار قدرتمند را ایجاد می‌کنند. اگر کسی در استخر یک بلاک معتبر پیدا کند، جایزه آن بلاک به طور مناسب بین تمام ماینرها، براساس هش‌ریتی که در آن مشارکت کرده‌اند، تقسیم می‌شود. این باعث می‌شود که حتی ماینرهای کوچک مثل ماینرهای فردی هم با توجه به میزان مشارکت‌شان در هش‌ریت، مقدار کمی جایزه دریافت کنند. برای ایجاد این سرویس، استخر بخشی از جایزه شما را می‌گیرد.

استخرهای استخراج می‌توانند باعث متمرکزشدن شوند، چون کاربران به سمت استخرهای بزرگتر می‌روند. نمودار زیر توزیع تقریبی استخرها را در ژانویه 2019 نشان می‌دهد.



حمله 51٪

تمرکز در استخرهای ماینینگ باعث نگرانی درمورد حمله 51٪ در شبکه می‌شود. اگر به نمودار بالا نگاه کنید، متوجه خواهید شد که مجموع هش‌ریت 5 استخر برتر نمودار، بیش از 50٪ کل شبکه است.

چنین حمله‌ای چگونه اتفاق می‌افتد و چه خطراتی به همراه دارد؟

وقتی بیش از 50٪ از هش‌ریت شبکه دراختیار شما باشد، می‌توانید بر ثبت بلاک‌ها در لجر اشراف کامل داشته باشید، چون توانایی شما در تولید زنجیره‌ی طولانی‌تر بیشتر از 50٪ از سایر اعضای شبکه است. توجه داشته باشید که اجماع ناکاماتو می‌گوید که باید زنجیره‌ای را بپذیریم که شامل طولانی‌ترین زنجیره از Proof of work باشد.

در اینجا مثالی ساده از نحوه رخ دادن حمله 51٪ ارائه می‌کنیم:

1. شبکه در کل 1000 هش در هرثانیه تولید می‌کند و بلاکچین را به‌روز می‌کند.
2. شما مقداری سخت‌افزار ماینینگ و برق خریداری می‌کنید که بتوانید 2000 هش برثانیه تولید کنید. حالا شما 66٪ از کل هش‌ریت را دراختیار دارید (2000/3000).
3. شما شروع به ماین کردن زنجیره‌ای می‌کنید که فقط شامل بلاک‌های خالی است.

4. دوهفته بعد زنجیره بلاک‌های خالیِ خود را در شبکه منتشر می‌کنید. چون شما توان ماین کردن، دوبرابر سریع‌تر از ماینرهای صادق را دارید، زنجیره شما دو برابر طولانی‌تر از بقیه شبکه خواهد بود. پس در تمام شبکه پذیرفته می‌شود و تاریخچه 2 هفته گذشته از بین خواهد رفت.

علاوه بر ماین کردن بلاک‌های خالی که زنجیره را بلااستفاده می‌کند، می‌توانید حمله Double Spend را هم ترتیب دهید:

1. تعدادی بیت کوین به یک صرافی ارسال کنید.
2. آن را با دلار مبادله کرده و دلار را برداشت کنید.
3. بعد از مدتی، زنجیره‌ای را که مخفیانه ماین کرده‌اید و پرداخت پول به صرافی در آن نوشته نشده است را، انتشار دهید.
4. شما حالا زنجیره را بازنویسی کرده‌اید و هم بیت کوین‌ها و هم دلارها را دردست دارید.

در عمل، با هش‌ریتی که امروزه وجود دارد، فراهم آوردن برق و سخت‌افزار لازم برای ترتیب دادن چنین حمله‌ای بسیار گران است. همچنین، نگذاشتن رد پا در حمله double spend با این روش بسیار سخت است. بجز اینها، شما باید به اندازه یک کشور متوسط انرژی مصرف کرده و میلیون‌ها دلار بابت خرید سخت‌افزار بپردازید، سپس میلیون‌ها دلار را برای مبادله به صرافی ارسال کنید. انجام چنین حمله‌ای در هیچ زمانی معقول نیست و اگر افرادی با بودجه نامحدود تصمیم به انجام این کار داشته باشند و بتوانند این حمله را در حد وسیعی اجرا کنند، شبکه رویکرد متفاوتی را برای Proof of work (نه sha 256) درنظر خواهد گرفت و سازگار خواهد شد، به‌گونه‌ای که تمام سخت‌افزارهای ASIC که توسط مهاجم استفاده شده‌اند بی‌فایده شوند. اگرچه این گزینه بلافاصله باعث ناکارآمد شدن تمام ماینرهای صادق نیز می‌شود اما شبکه زنده می‌ماند و از خاکستر خواهد برخاست.

علاوه بر غیرقابل اجرا بودن حمله، دردست داشتن اکثریت هش‌ریت به شما حق انجام هیچ‌یک از موارد زیر را نمی‌دهد:

1. شما نمی‌توانید از هوا سکه ایجاد کنید. این‌کار باعث نقض قانون جایزه بلاک‌ها می‌شود و حتی اگر بلاک دارای proof of work کافی باشد رد خواهد شد.
2. سکه‌هایی را که مالکش نیستید را نمی‌توانید خرج کنید، چون باید یک امضای دیجیتال معتبر ارائه دهید.

3. شما نمی‌توانید سرعت عرضه بیت کوین را بالا ببرید، چون سختی همیشه در هر 2016 بلاک تنظیم می‌شود.

درنتیجه، گره‌هایی که بیت کوین را به عنوان یک روش پرداخت پذیرفته‌اند، می‌توانند شبکه را صادق نگه دارند، حتی اگر اکثریت ماینرها خرابکار باشند. علاوه بر این نباید تصور کنیم که اگر یک استخر ماینینگ درصد خاصی از هش‌ریت را دراختیار دارد پس تمام سخت‌افزار لازم برای این حجم از هش‌ریت را دارد. درواقع استخرها ترکیبی از هزاران ماینر شخصی هستند. اگر استخر شروع به انجام رفتارهای نادرست کند، ماینرها می‌توانند استخر استخراج خود را عوض کنند؛ چراکه خواهان حفظ ارزش اقتصادی بیت کوین هستند. ماینرها برای کسب درآمد تلاش می‌کنند نه برای ازدست دادن آن.

در تاریخ سابقه‌ی ترک استخرهای بسیار قوی توسط ماینرها وجود دارد: در سال 2014، Ghash.io نزدیک به نیمی از قدرت شبکه را دردست داشت. ماینرها متوجه شدند که شبکه به سمت متمرکز شدن درحال حرکت است، پس داوطلبانه استخر را ترک کردند.

اگرچه امروزه استخرهای ماینینگ نسبتا متمرکز وجود دارد، اما ارتقاء مداوم تکنولوژی ماینینگ شامل طرحی به نام BetterHash است که به ماینرها این امکان را می‌دهد تا بر آنچه که ماین می‌کنند کنترل بیشتری داشته باشند و وابستگی آنها به هماهنگی استخر را کاهش می‌دهد.

Hard Fork ها و Soft Fork ها

پیچیده‌ترین موضوع در بیت کوین را در آخر مطرح می‌کنیم.

متوجه شدیم که نرم‌افزار بیت کوین چطور قوانینی که افراد بر آن توافق دارند را اجرا می‌کند و فهمیدیم که چگونه افراد برای اجرای قوانینی که موافق آن هستند تصمیم می‌گیرند که کدام نرم‌افزار را اجرا کنند.

همچنین توضیح دادیم که ماینرها درمورد قوانینی که درهنگام تولید بلاک رعایت می‌کنند، تصمیم می‌گیرند، و باید بلاک‌ها را به گونه‌ای که کاربران می‌خواهند ماین کنند، در غیر این صورت باید ریسک رد شدن بلاک و نگرفتن جایزه را بپذیرند.

درنهایت، می‌دانیم که نرم‌افزار بیت کوین طولانی‌ترین زنجیره از proof of work های معتبر را به عنوان زنجیره معتبر می‌پذیرد، و می‌دانیم که این چندگانگی در تعداد زنجیره‌ها (از این به بعد به این اتفاق فورک می‌گوییم) به این دلیل است که ماینرها زنجیره‌های تاریخ‌گذشته را ماین می‌کنند.

حالا بیایید به فورک‌هایی که عمدی ایجاد می‌شوند بپردازیم. فورکِ عمدی زمانی‌ست که تعدادی از ماینرها یا کاربران با قوانین جاری بیت کوین موافق نباشند. به‌طور کلی دو نوع فورک برای تغییر قوانین وجود دارد: Soft fork که سازگار با قبل است، و Hard fork که سازگار با قبل نیست. ببینیم این فورک‌ها چطور اتفاق می‌افتند و مثال‌هایی از آنها را مطرح کنیم.

Soft Fork

Soft fork تغییرات سازگار با گذشته در قوانین اجماع بیت کوین است. این به چه معناست؟ یعنی اگر شما یک گره قدیمی را اجرا کنید که به‌روزرسانی نشده باشد، گره شما هنوز هم می‌تواند بلاک‌های معتبر را تولید کند. برای یک گره که با فورک جدید به‌روزرسانی شده است تمام بلاک‌هایی که قبلا نامعتبر بودند هنوز هم نامعتبر هستند اما حالا بعضی از بلاک‌های معتبر ممکن است نامعتبر درنظر گرفته شوند. اجازه دهید با مثال این موضوع را روشن‌تر کنیم:

12 سپتامبر 2010 قوانین جدیدی به نرم‌افزار بیت کوین معرفی شد: سایز بلاک‌ها حداکثر می‌تواند 1مگابایت باشد. این قانون برای مقابله با اسپم‌ها در بلاکچین ایجاد شد. قبل از این قانون، بلاک‌ها با هر سایزی قابل قبول بودند. با قانون جدید تنها بلاک‌های با اندازه کوچکتر قابل پذیرش شدند. اگر شما یک گره قدیمی را اجرا می‌کردید که به‌روزرسانی نشده بود بلاک‌های کوچکتر هنوز هم معتبر بودند، پس شما تحت تاثیر قرار نمی‌گرفتید.

soft fork یک روش بدون تداخل برای به‌روزرسانی سیستم است؛ چراکه به اجراکنندگان گره‌ها این امکان را می‌دهد که داوطلبانه و به مرور زمان به نرم‌افزار جدید به‌روز شوند. اگر به‌روز هم نشوند می‌توانند مثل قبل به فعالیت خود ادامه دهند. فقط ماینرها که بلاک‌ها را تولید می‌کنند باید به‌روزرسانی کنند تا بلاک‌های تولیدشده از قوانین جدید پیروی کنند. وقتی یک ماینر قانون 1مگابایت را در فورک جدید به‌روزرسانی می‌کرد، سایز تمام بلاک‌های بعد از آن حداکثر 1 مگابایت بود. کاربرانی که نسخه‌های قدیمی نرم‌افزار را اجرا می‌کردند در این مورد آگاهی نداشتند.

Hard Fork

هارد فورک نقطه مقابل سافت فورک است. هارد فورک سازگار با گذشته نیست، تغییری است که در آن بلاک‌هایی که دراصل نامعتبر بودند حالا به عنوان بلاک معتبر درنظر گرفته می‌شوند. در هارد فورک گره‌های قدیمی که به‌روزرسانی نمی‌کردند دیگر نمی‌توانستند بلاک‌هایی را که تحت قوانین جدید ایجاد شده بودند را بررسی کنند. به همین دلیل یا باید در همان بلاکچین قدیمی می‌ماندند و یا نرم‌افزار خود را به‌روز می‌کردند. یکی از نمونه‌های هارد فورک تغییر سایز بلاک‌ها از 1 مگابایت به چیزی بزرگتر بود، یعنی بلاک‌هایی که تحت قانون قدیم تولید شده بودند حالا نامعتبر خواهند بود.

اکثر هارد فورک‌هایی که موافقت همه گره‌ها را دارند، در شبکه مشکلی ایجاد نمی‌کنند. همه گره‌ها باید سریعا قوانین را به‌روزرسانی کنند. اگر بعضی افراد متوجه به‌روزشدن قوانین نشوند، دیگر بلاک جدید دریافت نخواهند کرد و قاعدتا متوجه می‌شوند که نرم‌افزار ازکار افتاده است پس وادار به ارتقاء نرم‌افزار خود خواهند شد.

هارد فورک‌ها درعمل به این سادگی پیش نمی‌روند. در یک سیستم آنارشیستی و غیرمتمرکز، نمی‌توان همه را وادار به استفاده از قوانین جدید کرد. در اگوست 2017، افرادی که در رابطه با نحوه پیشرفت بلاکچین ناراضی بوده و خواهان پرداخت با کارمزد کمتری بودند، تصمیم گرفتند برای ایجاد زنجیره‌ای با بلاک‌های بزرگتر فورک ایجاد کنند. چون قانون بیت کوین تولید بلاک‌هایی کمتر از 1 مگابایت بود (با توجه به سافت فورک سال 2010)، این افراد تصمیم گرفتند زنجیره جدیدی ایجاد کنند که در آن اندازه بلاک‌ها بزرگتر باشد. این فورک به عنوان Bitcoin Cash شناخته شده است.

هارد فورکی مثل بیت کوین‌کش که از جانب همه گره‌ها و ماینرها پذیرفته نمی‌شود، یک بلاکچین جدید ایجاد می‌کند که قسمتی از تاریخچه آن با بلاکچین اولیه مشترک است، اما از نقطه‌ی تقسیم بلاکچین به بعد، سکه‌هایی که در فورک تولید می‌شوند دیگر بیت کوین نیستند و لذا توسط هیچ گرهی در شبکه بیت کوین قابل پذیرش نیستند.

موضوعِ بیت کوین‌بودن یا نبودن این سکه‌ها در سالهای بعد از بیت کوین‌کش بسیار بحث داغی بود. بعضی از افرادی که طرفدار بیت کوین‌کش بودند، اعتقاد داشتند که بیت کوین باید براساس آنچه که ساتوشی 10 سال پیش در مقاله اولیه خود نوشته است، تعریف شود، و برای اثبات نظر خود جملاتی از مقاله را گلچین کرده بودند. اما یک سیستم مبتنی بر اجماع براساس مشاجره‌هایی که در شبکه‌های اجتماعی شکل می‌گیرند کار نمی‌کند، بلکه براساس انتخاب افراد در اجرای نرم‌افزاری خاص، برای اجرای قوانین خاص عمل می‌کند.

درمورد این فورک، اکثریت افرادی که گره‌های مهم اقتصادی را اجرا می‌کردند- که کیف پول‌ها، صرافی و پذیرنده‌های بیت کوین بودند- نمی‌خواستند نرم‌افزار خود را، برای چیزی که گروه کمتری از آن حمایت می‌کنند و تیم کم‌تجربه‌تری آن را توسعه داده است و همین‌طور میزان هش‌ریت کم آن نشان می‌داد افراد کمتری خواهان تغییر این قوانین هستند، تغییر دهند. همچنین افراد فکر می‌کردند که چنین ارتقایی ارزش برهم زدن اکوسیستم را ندارد. مشکل هارد فورک‌ها این است که آنها زمانی موفق هستند که همه به آن سوییچ کنند، ولی اگر اختلاف نظر به‌وجود بیاید، دو کوین متفاوت ایجاد می‌شود. پس بیت کوین همان بیت کوین می‌ماند و بیت کوین‌کش، کوین جداگانه‌ای خواهد بود.

امروزه تعداد زیادی فورک بیت کوین ایجاد شده است، مثل Bitcoin Gold، Bitcoin Diamond و Bitcoin Private، که هش‌ریت کمتری امنیت آنها را تامین می‌کند و توسعه‌دهندگان کمتری از آنها پشتیبانی می‌کنند و تقریبا فعالیت اقتصادی ندارند. بسیاری از آنها به طور واضح اسکم و یا به احتمال کمی پروژه‌های تحقیقاتی هستند. صدها کوین شبیه به بیت کوین وجود دارند که کدهای مشابهی دارند اما تاریخچه حساب بیت کوین (UTXO مجموعه) را ندارند، مثل Litecoin و Dogecoin.

بازار آزاد

درباره کارمزد در فصل 5 مختصر صحبت کردیم، اما نیاز به بحث بیشتری دارد. در برنامه عرضه بیت کوین، هر 4 سال یک‌بار مقدار پاداش ماین کردن بلاک‌ها نصف می‌شود تا زمانی‌که کاملا حذف شود و بیت کوین درنهایت به حالت بدون پاداش درمی‌آید. به همین دلیل به روشی نیاز داریم تا انگیزه کافی به ماینرها بدهیم تا امنیت شبکه را همچنان تامین کنند.

کارمزد توسط بازار آزاد تعیین می‌شود، جایی‌که در آن کاربران برای خرید فضا در بلاک قیمت پیشنهاد می‌دهند. کاربرانی که تراکنش انجام می‌دهند، مشخص می‌کنند که چه مقدار کارمزد می‌خواهند به ماینرها پرداخت کنند، و ماینرها با توجه به مقدار کارمزد تصمیم می‌گیرند که تراکنش آنها را در بلاک قرار بدهند یا نه. زمانی که تعداد تراکنش‌های درصف‌انتظار کم باشد، مقدار کارمزد می‌تواند درحد کمی تعیین شود چون رقابتی وجود ندارد. اما با پر شدن فضای بلاک، کاربرانی که می‌خواهند تراکنش‌شان سریع‌تر تایید شود مقدار کارمزد بیشتر، و کسانی که عجله‌ای ندارند کارمزد کمتری پرداخت می‌کنند و زمان بیشتری هم منتظر می‌مانند تا فضای بلاک خالی و تراکنش انجام شود.

برخلاف سیستم مالی سنتی، که در آن مقدار کارمزد درصدی از مبلغ مورد انتقال است، در بیت کوین مبلغ منتقل‌شده بر کارمزد هیچ تاثیری ندارد. درعوض، کارمزد متناسب با فراوانی منابع مصرفی که همان فضای بلاک است، تعیین می‌شود. بنابراین کارمزد با "ساتوشی بر بایت" اندازه‌گیری می‌شود (هر بایت برابر با 8 بیت است، درواقع فقط اندازه‌گیری مقدار داده در تراکنش شما است). درنتیجه تراکنشی که یک میلیون بیت کوین را به یک آدرس ارسال می‌کند ارزان‌تر از تراکنشی است که یک بیت کوین را بین 10 حساب بخش می‌کند، چون دومی فضای مصرفی بیشتری در بلاک نیاز دارد.

در گذشته، در برهه‌ای از زمان که بیت کوین متقاضی زیادی داشت، مثل زمان افزایش قیمت اواخر سال 2017، کارمزدها بسیار بالا رفت. بعد از آن امکانات جدیدی برای کاهش فشار کارمزد در شبکه پیاده شد.

یکی از این امکانات به‌نام Segregated Witness یا Segwit است که با جدا کردن امضای دیجیتال از تراکنش‌ها و ایجاد فضای بیشتر برای داده‌ها، قرارگیری داده‌ها در بلاک را سازماندهی کرد- تراکنش‌هایی که از این به‌روزرسانی استفاده می‌کنند، بیش از یک مگابایت از فضای بلاک را از طریق این ترفند هوشمندانه استفاده می‌کنند که توضیح آن در حوصله این کتاب نیست.

کاهش کارمزد از طریق دسته‌بندی نیز اتفاق افتاد: صرافی‌ها و سایر گروه‌های تاثیرگذار در اکوسیستم، تراکنش‌های چندین کاربر بیت کوین را در یک تراکنش ترکیب کردند، برخلاف سیستم پرداخت سنتی در بانک یا PayPal که تراکنش‌ها از یک فرد به فرد دیگر است. یادآوری می‌کنم که یک تراکنش بیت کوین می‌تواند تعداد زیادی ورودی را با هم ترکیب کند و تعداد زیادی خروجی تولید کند. بنابراین یک صرافی که باید برای 100 نفر بیت کوین ارسال کند، این کار را در یک تراکنش انجام می‌دهد. این روش، استفاده از فضای بلاک را بهینه‌تر می‌کند و به جای انجام تعداد کمی تراکنش در هرثانیه، هزاران پرداخت در ثانیه انجام می‌شود.

Segwit و دسته‌بندی هم‌اکنون برای کاهش تقاضا برای فضای بلاک به‌خوبی استفاده می‌شوند. پیشرفت‌های بیشتری برای استفاده بهینه از فضای بلاک درحال شکل‌گیری است. با این‌حال زمانی خواهد رسید که کارمزد بیت کوین به دلیل پر شدن بلاک‌ها در اثر تقاضای زیاد کاربران، دوباره بالا خواهد رفت.

تحولات آینده در بیت کوین

حالا به اختراع پروتکل‌ها، و چگونگی تکامل شبکه درطول زمان می‌پردازیم؛ به آینده نگاه می‌کنیم و برخی پیشرفت‌هایی که به‌زودی برای بیت کوین حاصل می‌شود را بررسی می‌کنیم.

برخلاف ارز سنتی، که چاپ و استفاده می‌شود، بیت کوین یک پول قابل برنامه‌نویسی است که در آن می‌توان خدمات زیادی ایجاد کرد. این یک مفهوم کاملا جدید است که ما فقط گوشه‌ای از آن را نشان دادیم.

شبکه Lightning

همان‌طور که گفته شد، بیت کوین مشکل افزایش کارمزد با افزایش تقاضا برای فضای خالی در بلاک‌ها را دارد. امروزه بیت کوین توانایی انجام 3 تا 7 تراکنش درثانیه براساس تعداد تراکنش‌هایی که می‌توانند در بلاک قرار گیرند را دارد. به یاد داشته باشید که اگرچه هر تراکنش می‌تواند از طریق دسته‌بندی، درواقع پرداخت به صدها نفر باشد اما هنوز هم ظرفیت کافی برای تبدیل شدن به یک شبکه پرداخت سراسری را ندارد.

یک راه حل ساده می‌تواند برای افزایش سایز بلاک وجود داشته باشد و چندین رقیب بیت کوین مثل بیت کوین‌کش این روش را امتحان کرده‌اند. اما بیت کوین این کار را انجام نمی‌دهد چون افزایش اندازه بلاک می‌تواند بر خصوصیات غیرمتمرکز شبکه مثل تعداد گره‌ها و پراکندگی جغرافیایی آنها تاثیر منفی بگذارد. حتی اگر افزایش سایز بلاک با ارتقاء سخت‌افزار ممکن می‌شد، این مسئله وجود دارد که ماهیت بیت کوین غیرمتمرکز است یعنی هارد فورک‌هایی که تلاش کردند تا سایز بلاک را تغییر دهند، باعث انشعابات زیادی شده و به یک کوین جدید تبدیل شدند.

همچنین افزایش سایز بلاک‌ها مشکل مناسب نبودن بیت کوین به عنوان یک سیستم پرداخت جهانی را نیز حل نمی‌کند، زیرا به سادگی مقیاس‌پذیر نمی‌شود. وارد شبکه lightning می‌شویم: یک پروتکل دیگر و مجموعه‌ای از روش‌های نرم‌افزاری که تراکنش‌های بیت کوینی را به صورت off-chain (خارج از زنجیره بیت کوین) ایجاد می‌کند.

شبکه lightning به تنهایی می‌تواند عنوان یک کتاب باشد، اما توضیح مختصری درباره آن می‌دهیم.

ایده لایتنینگ این است که هر تراکنشی نیاز به ثبت در بلاکچین ندارد. برای مثال اگر من و شما برای خرید نوشیدنی در یک کافه باشیم می‌توانیم یک صورت‌حساب باز کنیم و تا آخر شب آنجا بمانیم. اصلا جالب نیست که برای هر نوشیدنی که سفارش می‌دهیم کارت اعتباری را عوض کنیم چراکه اتلاف وقت است. در بیت کوین، صرف انرژی برابر با کل یک کشور برای تایید خرید نوشیدنی و ثبت این خرید در هزاران کامپیوتر در سراسر جهان نه مقیاس‌پذیر است و نه برای حفظ حریم خصوصی خوب است.

اگر شبکه لایتنینگ موفق شود، نکات منفی زیادی در بیت کوین رفع خواهد شد:

- توان عملیاتی تقریبا نامحدود: صدها و هزاران تراکنش کوچک بیت کوین می‌توانند انجام شود و سپس یکبار به عنوان پرداخت نهایی در بلاکچین بیت کوین ثبت شود.
- تاییدهای سریع: نیاز نیست صبر کنیم تا بلاک‌ها ماین شوند.
- تراکنش‌هایی که کارمزد بسار کمی دارند برای پرداخت‌های کم مناسب هستند، مثل پرداخت یک پنی برای خواندن یک وبلاگ.
- بیشتر شدن حریم خصوصی: فقط افرادی که در تراکنش شرکت می‌کنند می‌توانند از پرداخت ما مطلع شوند، درست برعکس تراکنش‌های on-chain که تراکنش درسراسر جهان پخش می‌شود.
- لایتنینگ از مفهوم کانال پرداخت استفاده می‌کند، که درواقع همان تراکنش‌های onchain هستند که مبلغی بیت کوین در آن بلوکه می‌شود و سپس توسط شبکه لایتنینگ سریع و تقریبا رایگان انتقال داده می‌شود. شبکه لایتنینگ در مراحل اولیه است اما با این وجود نویدبخش است. می‌توانید سایت https://yalls.org/ را که از لایتنینگ استفاده می‌کند را ببینید.

بیت کوین در فضا

بیت کوین برای مقاومت دربرابر سانسور کار خوبی انجام داده است، همان‌طور که دربرابر دزدی مقاوم است (می‌توانید در ذهن خود نگهداری کنید)، و دربرابر سانسور جابه‌جایی بیت کوین نیز مقاوم است چون تنها یک ماینر صادق کافی است تا تراکنش ما تایید شود (خود شما هم می‌توانید ماین کنید).

با این حال چون بیت کوین از طریق اینترنت جابه‌جا می‌شود، درمعرض سانسور در سطح شبکه است. دولت‌ها اگر بخواهند فعالیت بیت کوین را کاهش دهند می‌توانند ترافیک بیت کوین را برای ورود به کشورشان مسدود کنند.

ماهواره‌ی "بلاک استریم" اولین تلاش برای حذف سانسور در شبکه و همچنین دسترسی به مناطق دورافتاده‌ای که به اینترنت متصل نیستند، می‌باشد. این ماهواره به همه این امکان را می‌دهد که با یک دیش و یک سری تجهیزات ارزان به شبکه بیت کوین متصل شوند و بلاکچین را دانلود کنند، که ارتباط دوطرفه به زودی امکان‌پذیر خواهد شد. تلاش‌های دیگری مثل TxTenna برای ساخت شبکه مش مستقل نیز وجود دارند.

فصل 10: و اما بعد چه؟

تمام ماجرا همین بود، مراحل اختراع بیت کوین را دیدید و یاد گرفتید، حالا آماده برای تحقیقات بیشتر هستید.

بعد از این کتاب سراغ چه می‌روید؟ در اینجا تعدادی منبع برای مطالعه بیشتر معرفی شده‌اند:

برای یادگیری بیشتر درباره اقتصاد پشت پرده بیت کوین:

- The Bitcoin Standard by Saifedean Ammous
- Cryptoassets by Chris Burniske and Jack Tatar
- Google: Austrian Economics

Bitcoin Investment Theses by Pierre Rochard
https://medium.com/@pierre_rochard/bitcoin-investmenttheses-part-1-e97670b5389b

- The Bullish Case for Bitcoin by Vijay Boyapati

https://medium.com/@vijayboyapati/the-bullish-case-forbitcoin-6ecc8bdecc1

برای درک بیشتر در دانش کامپیوتری :

- وایت‌پیپر بیت کوین نوشته ساتوشی ناکاماتو
https://bitcoin.org/bitcoin.pdf
- Mastering Bitcoin by Andreas Antonopulous

Jimmy Song's seminar at https://programmingblockchain.com/ and his book on github at https://programmingblockchain.gitbook.io/programmingblockchain

برای آموزش بیشتر درباره تاریخچه و فلسفه بیت کوین:

- Planting Bitcoin by Dan Held
https://medium.com/@danhedl/planting-bitcoin-soundmoney-72e80e40ff62
- Bitcoin Governance by Pierre Richard
https://medium.com/@pierre_rochard/bitcoin-governance37e86299470f
- Bitcoin Past and Future by Murad Mahmudov
https://blog.usejournal.com/bitcoin-past-and-future-45d92b3180f1
- Every video made by Andreas Antonopulous, especially Currency Wars and The Monument of Immutability, at https://www.youtube.com/user/aantonop

بخش بزرگی از اکوسیستم بیت کوین در توییتر است، در اینجا تعدادی از افرادی که دنبال کردن آنها مفید است ذکر شده‌اند:

```
@lopp
@pwuille
@adam3us
@danheld
@TraceMayer
@pierre_rochard
@bitstein
@Melt_Dem
@theonevortex
@WhatBitcoinDid
@stephanlivera
@TheBlock__
@TheLTBNetwork
@real_vijay
@jimmysong
@Excellion
@starkness
@roasbeef
@saifedean
@giacomozucco
@Snyke
@aantonop
@MustStopMurad
@peterktodd
@skwp
```

می‌توانید نوشته‌های بیشتری را در yanpritzker.com پیدا کنید.

تشکر و قدردانی

از همه کسانی که در زمان نوشتن این کتاب نظر خود را ارایه دادند متشکرم به خصوص:
Walter Rosenberg و Jonathan Wheeler ،Pritzker، Yury، Phil Geiger، Joe Levering
از Jimmy Song به خاطر سمینار برنامه‌نویسی بلاکچین، که به من انگیزه لازم برای جمع‌آوری این متن را داد ممنونم.

درباره نویسنده

Yan Pritzker در 20 سال گذشته یک توسعه‌دهنده نرم‌افزار و کارآفرین بوده است. از سال 2012 تا 2018 او CTO سایت Reverb.com بوده و تکنولوژی و زیرساخت‌ها را مدیریت کرده است. امروزه او تمرکز خود را بر آموزش بیت کوین و مشاوره برای استارت‌آپ‌های نوپا گذاشته است.

مطالب نویسنده درباره بیت کوین و موضوعات مرتبط در سایت yanpritzker.com

همچنین می‌توانید در توییتر نیز او را دنبال کنید:@skwp