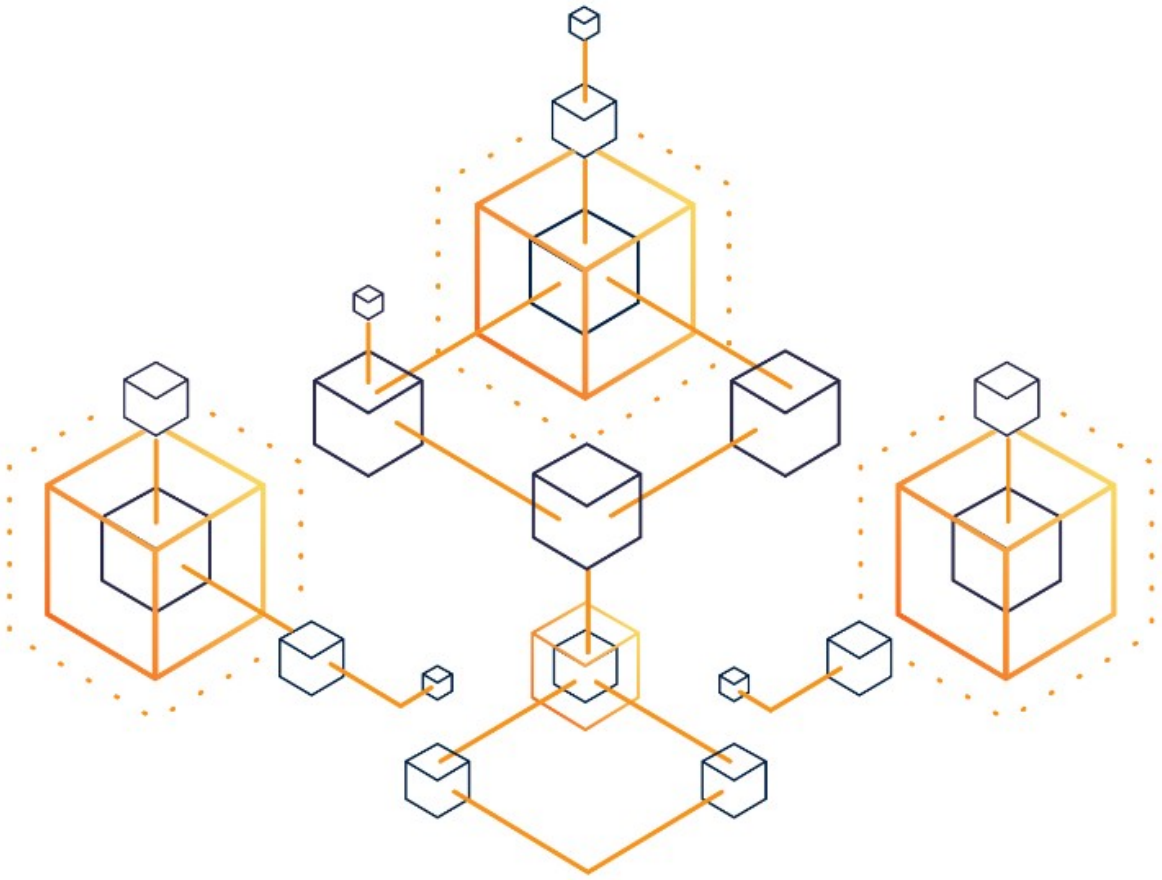
کوین ایران
CoinIran

اختراع
بیت‌کوین



ویراست سوم

سایت منابع فارسی بیت‌کوین

سخنی با خوانندگان

این کتاب نحوه کار شبکه بیت‌کوین را به زبانی ساده توضیح می‌دهد و تلاش می‌کند بیت‌کوین را قدم به قدم و با همراهی خواننده اختراع کند. پیش‌نیاز مطالعه این کتاب به گفته نویسنده، ریاضیات دبیرستان است.

ممکن است شما به‌عنوان فردی که بخشی از دارایی خود را در بیت‌کوین سرمایه‌گذاری کرده است معتقد باشید به درک نحوه کار شبکه بیت‌کوین نیازی پیدا نخواهید کرد. یا از نحوه کار با کیف پول‌های بیت‌کوین شناخت کلی دارید و نیازی به عمیق‌تر شدن در مفاهیم بیت‌کوین احساس نمی‌کنید. در این مقدمه کوتاه توضیح می‌دهیم که چرا همه افرادی که به نوعی با بیت‌کوین سر و کار دارند باید به‌طور کلی از ساز و کار شبکه بیت‌کوین اطلاع داشته باشند.

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 سایت منابع فارسی بیت‌کوین موجود 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 تأییدکننده در سراسر

1 Digital Scarcity
2 The Little Bitcoin Book

دنیا تراکنش‌های شبکه بیت‌کوین را مورد بازبینی قرار می‌دهند و تاریخچه همه تراکنش‌ها را در خود ذخیره می‌کنند. اسم این تأیید کننده‌ها فول نود[1] است. (نرم‌افزار بیت‌کوین که هرکس می‌تواند با اجرای آن اعتبار تراکنش‌های بیت‌کوین را بازبینی، و از درستی آن اطمینان حاصل کند)

ماینرها[2] (فرد یا گروهی که از دستگاه‌های مخصوصی برای ساختن بلاک‌های جدید در شبکه بیت‌کوین استفاده می‌کنند) در سراسر 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[3]» نوشته‌اند. تراکنش‌هایی که داخل بلاک‌های بیت‌کوین قرار می‌گیرند را کاربران بیت‌کوین با استفاده از نرم‌افزارهای کیف‌پولشان ساخته‌اند.

"همه این اجزاء 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[4] 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

1 Full Node
2 Miner
3 Core Developers
4 User Activated Soft Fork

> 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.
>
> – بخشی از کتاب کوچک بیت‌کوین

پس اجازه تغییر قوانین بیت‌کوین تنها در دست اعضای این شبکه است و این وظیفه‌ای است بسیار مهم بر دوش همه بیت‌کوینرهای سراسر دنیا فارغ از نژاد، منطقه جغرافیایی، زبان، و مسائل سیاسی. 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 برای آگاهی‌بخشی عمومی، همچنین رسانه خبری-آموزشی کوین‌ایران بابت بازبینی و صفحه‌بندی ویراست اول این کتاب، تشکر و قدردانی می‌کنیم.

bitcoind.me
منابع فارسی بیت‌کوین
ویراست دوم - زمستان ۱۳۹۹

بیت‌کوین، پول مردمی از طرف مردم برای مردم

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

کتاب حاضر تحت عنوان **اختراع بیت‌کوین** (Inventing Bitcoin) است که نسخه اصلی آن در سال ۲۰۱۹ منتشر گردیده است. نویسنده این کتاب آقای یان پریتزکر (Yan Pritzker) است. او در ۲۰ سال گذشته یک توسعه‌دهنده نرم‌افزار و کار آفرین بوده است. همچنین از سال ۲۰۱۸ به‌عنوان مدیر تکنولوژی سایت Riverb.com وظیفه مدیریت تکنولوژی و زیرساخت‌ها 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 است که در این زمینه کتاب‌های 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 بیت‌کوین به عنوان جذابترین اختراع زمانه درگیر نماید. بنابراین مطالعه این کتاب به افرادی که تاکنون هیچ آشنایی با بیت‌کوین ندارند و یا کسانی که آشنایی ابتدایی دارند، توصیه می‌شود.

مترجم این کتاب که هویت وی با شناسه کاربری nodrunner در توئیتر شناخته می‌شود با کلید 6137-661C-6B65-933B نسخه اولیه ترجمه این کتاب را در اختیار کوین‌ایران قرار داده است تا با کمک تحریریه کوین‌ایران 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 **کوین‌ایران** امیدوار است که با ارائه این کتاب گام دیگری در جهت آگاه‌سازی و آشنایی جامعه مخاطب فارسی زبان برداشته و به آن‌ها یاری رساند.

مقدمه نویسنده

به کتاب اختراع بیت‌کوین خوش آمدید. هدف من در این کتاب تحلیل اقتصادی بیت‌کوین نیست، همچنین قصد ندارم شما را متقاعد کنم که بیت‌کوین طلای دیجیتال است. برای این منظور کتاب پول‌طلا[1] نوشته سیف‌الدین اموس[2] را معرفی می‌کنم.

قرار نیست از زاویه سرمایه‌گذاری به بیت‌کوین نگاه کنم و یا دلیل بیاورم که هر فرد باید حداقل مقدار کمی بیت‌کوین داشته باشد. قصدِ بررسی چارت‌ها و تاریخچه قیمت بیت‌کوین را هم ندارم. اگر به دنبال این موضوعات هستید کتاب دارایی دیجیتال[3] نوشته کریس برنیسکه[4] و جک تاتار[5] را پیشنهاد می‌کنم.

همینطور ما به دنبال کاوش در نحوه عملکرد پروتکل بیت‌کوین در لایه‌های عمیق آن نیستیم، قصد بررسی کُدهای کامپیوتری را هم نداریم. کتاب تسلط بر بیت‌کوین[6] نوشته اندریاس انتنوپولوس[7] برای این منظور مناسب‌تر است.

1 The Bitcoin Standard
2 Saifedean Ammous
3 Cryptoassets
4 Chris Burniske
5 Jack Tatar
6 Mastering Bitcoin
7 Andreas Antonopoulos

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

بیشتر افراد، اولین باری که اسم بیت‌کوین را می‌شنوند، از آن سر در نمی‌آورند. آیا بیت‌کوین پول جادویی اینترنتی است؟ از کجا آمده؟ چه کسی آن را کنترل می‌کند؟ چرا به این اندازه مهم است؟

من از درک تمام چیزهایی که کنار هم جمع شده‌اند تا بیت‌کوین را بسازند (فیزیک، ریاضیات، رمزنگاری، نظریه بازی، اقتصاد و علوم کامپیوتر) بسیار لذت بردم. تلاش می‌کنم در این کتاب دانش خود را به زبان بسیار ساده و قابل درکی به شما انتقال دهم.

برای انتقال بهتر مفاهیم، قدم به قدم پیش می‌رویم و تنها پیش‌نیاز درک مطالب این کتاب، ریاضیات دبیرستان است. ما قدم به قدم بیت‌کوین را اختراع می‌کنیم. امیدوارم این کتاب انگیزه لازم برای ورود به دنیای بیت‌کوین را در شما ایجاد کند. خوب، بیایید شروع کنیم!

فصل اول

بیت‌کوین چیست؟

بیت‌کوین یک پول الکترونیکی نظیر به نظیر[1] است؛ یک پول دیجیتال که می‌تواند بین افراد و کامپیوترها بدون واسطه (مثل بانک) جابه‌جا شود و تولید 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، لازم نیست طرف مقابل شما را بشناسد. کافی است مطمئن شود پولی که از شما گرفته است جعلی نیست، که اغلب برای پول‌های فیزیکی با نگاه کردن و لمس پول این اطمینان حاصل می‌شود.

با توجه به دیجیتالی شدن جوامع، امروزه بیشترِ پرداخت‌های ما دیجیتالی، اینترنتی، و با استفاده از سرویس‌های یک شرکت یا نهاد واسط انجام می‌شود. این واسطه می‌تواند یک موسسه کارت اعتباری مثل ویزا[2] یا سرویس‌های پرداخت دیجیتال مانند پی‌پال[3] یا اپل پی[4] و یا پلتفرم‌های آنلاینی مثل وی‌چت[5] باشد. (در کشور ما هم واسطه‌های پرداخت زیادی وجود دارند که معمولاً خدمات خود را بر بستر اپلیکیشن‌های موبایل ارائه می‌دهند. - م)

1 Peer to Peer
2 Visa
3 Paypal
4 Apple Pay
5 WeChat

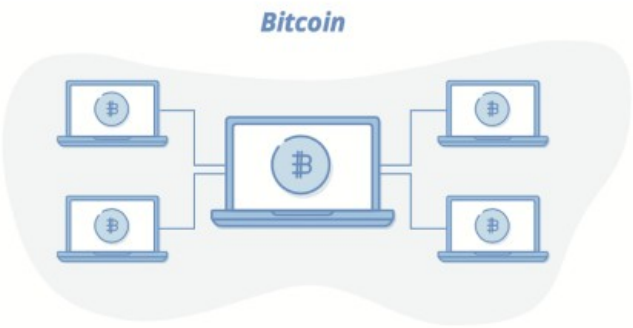
این نوع پرداخت دیجیتال، نیازمند اعتماد به یک کنترل‌کننده مرکزی است که هر پرداخت را بررسی و تأیید کند، چون پولی را که یک فرد می‌توانست با لمس کردن و دیدن، از جعلی نبودن آن اطمینان حاصل کند حالا تغییر ماهیت داده و تبدیل به داده‌های دیجیتالی شده است و باید توسط مرجعی که نقل و انتقالات را کنترل می‌کند تایید شود. بیت‌کوین جایگزینی برای پول‌های دیجیتالیِ تحت کنترل مراجع مرکزی است، سیستمی که سه جزء اساسی دارد. در بخش بعد به شرح انگیزه‌هایی که در نحوه طراحی آن اثرگذار بوده‌اند خواهیم پرداخت.

۱. یک دارایی دیجیتال (معمولا `bitcoin` که با `b` کوچک نوشته می‌شود)، که به تعداد محدودی وجود دارد، برنامه عرضه آن از قبل مشخص شده و قابل تغییر هم نیست. این مسئله کاملاً برخلاف پولی است که ما امروزه استفاده می‌کنیم؛ چراکه پول‌ها توسط دولت‌ها و بانک‌های مرکزی عرضه می‌شوند و نرخ عرضه (چاپ) آنها درطول زمان غیرقابل پیش‌بینی است.

۲. یک گروه از کامپیوترهای متصل به یکدیگر (شبکه `Bitcoin` با `B` بزرگ)، که هرکسی می‌تواند به این شبکه وصل شود. این شبکه برای ردیابی مالکیت بیت‌کوین و انتقال آن بین اعضای شبکه به کار گرفته می‌شود و هرگونه واسطه‌ای اعم از بانک‌ها، موسسه‌های اعتباری و سرویس‌های پرداخت را حذف می‌کند.

۳. نرم‌افزار کاربران بیت‌کوین؛ کُدی که هرکسی می‌تواند آن را روی کامپیوترش اجرا کند تا عضوی از شبکه باشد. این نرم‌افزار متن باز[1] است، به این معنا که همه می‌توانند به کد آن دسترسی داشته باشند و نحوه کار آن را ببینند و به رفع اشکالات و افزودن قابلیت‌های جدید کمک کنند.

1 `Open Source`



بیت‌کوین از کجا آمده است؟

بیت‌کوین درسال ۲۰۰۸ توسط شخص یا گروهی اختراع شده است که با نام مستعار ساتوشی ناکاموتو[1] شناخته می‌شوند. هیچ‌کس از هویت واقعی این شخص یا گروه اطلاعی ندارد.

در ۱۱ فوریه ۲۰۰۹ ساتوشی نمونه اولیه بیت‌کوین را در یک گروه آنلاین متعلق به سایفرپانک‌ها[2] عرضه کرد؛ گروهی که روی فناوری رمزنگاری کار می‌کنند و دغدغه آنها دفاع از حریم خصوصی افراد است.

بخش‌هایی از نوشته‌های ساتوشی در زیر آمده است. در فصل بعد این جملات و انگیزه‌های او برای اختراع بیت‌کوین را توضیح خواهم داد.

> من یک سیستم پول الکترونیک[3] به نام بیت‌کوین ایجاد کرده‌ام که متن باز و نظیربه‌نظیر است. کاملا غیرمتمرکز است، بدون هیچ کنترل کننده مرکزی و یا

1 Satoshi Nakamoto
2 Cypherpunk
3 e-cash

واسطه قابل اعتماد؛ چراکه به جای اعتماد همه چیز بر اساس اثبات رمزنگاری[۴] پایه‌گذاری شده است.

مشکل ریشه‌ای پولی که در حال حاضر استفاده می‌کنیم، اعتمادی‌ست که برای عملکرد آن لازم است. برای حفظ ارزش پول راهی جز اعتماد به بانک مرکزی نداریم. اما تاریخ پولِ فیات[۱] پر از موارد نقض این اعتماد است. برای نگهداری و انتقال الکترونیکی پول‌های‌مان باید به بانک اعتماد کنیم، اما بانک‌ها روش بانکداری ذخیره کسری را اجرا می‌کنند و آن را در موج‌های حبابِ اعتبار، به شکل اعتبار قرض می‌دهند. ما باید درمورد حریم خصوصی خود به آنها اعتماد کنیم. به آنها اعتماد کنیم تا اجازه ندهند سارقان اطلاعات شخصی حساب ما را خالی کنند. هزینه‌های کلان آنها پرداخت‌های خُرد را غیرممکن می‌کند.

نسل قبلی سیستم‌های کامپیوتریِ چندکاربره قبل از پدید آمدن رمزنگاری قوی با چنین مشکلی روبرو بودند و کاربران برای حفظ امنیت فایل‌های خود متکی به کلمه عبور[۲] بودند [...]

سپس رمزنگاری‌های قوی ایجاد شدند و دردسترس همه قرار گرفتند و نیاز به اعتماد از بین رفت. داده‌ها می‌توانستند به نحوی ایمن شوند که به صورت فیزیکی برای هیچ‌کس، صرف‌نظر از دلیل و بهانه آن‌ها، قابل دستیابی نباشند.

حالا زمان آن فرا رسیده است که این اتفاق برای پول نیز رخ دهد؛ با پول الکترونیکی[۳] براساس اثبات رمزنگاری، بدون نیاز به اعتماد به شخص سوم یا یک واسطه، به صورت امن و بدون دردسر. [...]

4 Crypto Proof
1 Fiat Currencies
2 Password
3 e-currency

راه حل بیت‌کوین برای جلوگیری از دوبار خرج کردن[1] استفاده از یک شبکه نظیر به نظیر است. به طور خلاصه این شبکه شبیه به یک سرور زمان‌سنج توزیع شده[2] کار می‌کند که اولین تراکنش را برای خرج کردنِ یک کوین(سکه)[3] برچسب زمانی می‌زند. این روش از ویژگی اطلاعات بهره می‌برد؛ به آسانی منتشر می‌شود ولی سرکوب آن دشوار است. برای جزئیات بیشتر به سایت http://www.bitcoin.org/bitcoin.pdf مراجعه کنید.

– ساتوشی ناکاموتو

زمانی که بیت‌کوین راه‌اندازی شد، تعداد انگشت‌شماری از آن استفاده کردند. آنها شبکه بیت‌کوین را روی کامپیوترهای‌شان (که به آن نود[4] می‌گویند) اجرا کردند تا شبکه قدرتمندتر شود. بیشتر افراد فکر می‌کردند بیت‌کوین شبیه به یک شوخی است و در آینده نقایص جدی در آن پیدا خواهد شد و نمی‌تواند موفق شود.

در طول زمان افراد بیشتری به شبکه بیت‌کوین پیوستند، از کامپیوترهای‌شان برای افزایش امنیت شبکه استفاده کردند و با مبادله بیت‌کوین با کالا، خدمات، یا ارزهای دیگر، ارزش بیشتری به آن دادند. امروز، بیش از ۱۰ سال از ارائه بیت‌کوین می‌گذرد. میلیون‌ها نفر از بیت‌کوین استفاده می‌کنند، ده‌ها تا صدها هزاران نود نرم‌افزار رایگان و متن‌باز آن را اجرا می‌کنند، و کُد آن توسط صدها داوطلب و شرکت مختلف در سراسر جهان در حال بهبود و توسعه است.

بیت‌کوین اختراعی نبود که بدون هیچ پیش‌زمینه‌ای ساخته شود. در مقاله معرفی آن که ساتوشی ارائه داد، به چندین تلاش مهم برای ایجاد سیستم‌های مشابه بیت‌کوین اشاره شده

1 Double Spend
2 Distributed timestamp server
3 Coin
4 Node

است، مثل بی-مانی[1] که توسط وِی دای [2] و هش‌کش[3] که توسط آدام بک[4] معرفی شد. اختراع بیت‌کوین براساس چنین تلاش‌هایی صورت پذیرفت ولی با این حال بیت‌کوین به‌عنوان اولین سیستم غیرمتمرکزی که برای خلق و جابه‌جا کردن پول دیجیتال، تحت کنترل هیچ شخص یا نهادی نیست، اساساً بر اساس طرح ساده‌ای کار می‌کند.

بیت‌کوین چه مشکلی را حل می‌کند؟

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. در ادامه بحث از طریق تمرین و مثال‌های مختلف، این مفاهیم ناآشنا را هم متوجه خواهید شد.

من یک پول دیجیتالی نظیر به نظیر و متن‌باز ایجاد کرده‌ام

اینجا منظور از نظیر به نظیر همان بدون واسطه است، به این معنا که در یک سیستم هرکسی می‌تواند بدون هیچ واسطه‌ای با شخص دیگر ارتباط برقرار کند. شما ممکن است نمونه‌هایی از سیستم‌های اشتراک‌گذاری فایل مثل نپستر[5]، کازاء[6]، و بیت‌تورنت[7] را به‌خاطر آورید. بیت‌تورنت برای اولین بار این قابلیت را برای کاربرانش فراهم کرد که بدون نیاز به دانلود یک موزیک از یک وب‌سایت قادر باشند آن را با یکدیگر به اشتراک بگذارند. ساتوشی در طراحی بیت‌کوین این امکان را ایجاد کرده است که افراد بتوانند پول دیجیتال[8] را بدون واسطه با هم مبادله کنند.

1 b-money
2 Wei Dai
3 Hashcash
4 Adam Back
5 Napster
6 Kazaa
7 BitTorrent
8 e-cash

نرم‌افزارِ آن، متن‌باز است، یعنی هر کسی می‌تواند به کدهای نرم‌افزار دسترسی داشته باشد و چگونگیِ 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 کُد همه چیز را متوجه شویم و اگر چیزی باب میل ما نبود آن را تغییر دهیم. (در این مورد بیشتر صحبت خواهیم کرد.)

کاملا غیرمتمرکز است و نیازی به یک سرور مرکزی یا اعضای معتمد ندارد

ساتوشی ذکر می‌کند که سیستم غیرمتمرکز است تا آن را از سیستمی که نیاز به یک مرکز کنترل دارد متمایز کند. در تلاش‌های قبل برای ساختن پول دیجیتال، مثل دیجی‌کَش[1] که در سال ۱۹۸۹ توسط دیوید چاوم[2] ارائه شد، به یک سرور مرکزی شامل یک یا چند کامپیوتر نیاز بود که مسئول تایید پرداخت‌ها و خلق پول دیجیتال بودند و توسط یک شرکت مشخص اداره می‌شدند.

این پول‌های خصوصی که برای خلق و مدیریت پول تحت نظارت یک شرکت مرکزی فعالیت می‌کردند، محکوم به شکست بودند. افراد نمی‌توانند به پولی اعتماد کنند که درصورت توقف فعالیت یک شرکتِ به‌خصوص، یا هَک شدن، خرابی سِرورها، یا تعطیلی آن توسط دولت، از بین برود.

ماهیت غیرمتمرکز بیت‌کوین مفهوم پول نقد را به حوزه دیجیتال بازمی‌گرداند: می‌توان آن را بدون نیاز به صحبت کردن با کسی، یا اجازه گرفتن از کسی، در تمام طول شبانه‌روز و تمام ۳۶۵ روز سال، بدون نیاز به مراجعه به هیچ نهاد مرکزیِ مورد اعتمادی، منتقل کرد.

1 DigiCash
2 David Chaum

به جای اعتماد همه چیز بر مبنای اثبات رمزنگاری[1] است

بیت‌کوین چگونه 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 «آیدا» است و ۱۰هزارتومان در حساب بانکی خود دارد، می‌توان از محاسبات رمزنگاری برای اثبات این ادعا استفاده کرد، به نحوی که انجام آن ساده باشد. این قابلیت اساسِ سیستم بیت‌کوین است که هم مالکیت پول و هم امنیت شبکه را تأمین می‌کند.

درمورد حریم خصوصی باید به بانک‌ها اعتماد کنیم تا از موجودی حساب ما در مقابل سارقان اطلاعات شخصی محافظت کنند و اجازه ندهند آن‌ها حساب ما را خالی کنند

بیت‌کوین برخلاف حساب‌های بانکی، سیستم‌های پرداخت دیجیتال، یا کارت‌های اعتباری به افراد اجازه می‌دهد بدون نیاز به ارائه اطلاعات شخصی با هم دادوستد کنند.

مراکز اطلاعات متمرکزی که اطلاعات مشتریان بانک‌ها، شرکت‌های کارت اعتباری، سیستم‌های پرداخت، و دولت‌ها در آن‌ها ذخیره می‌شود برای هکرها بسیار جذاب هستند. هک شدن شرکت اعتباری اکوئیفکس[2] در سال ۲۰۱۷ و قرارگرفتن اطلاعات ۱۴۰ میلیون نفر در دست هکرها گواهی بر این سخن ساتوشی است.

هدف بیت‌کوین 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 پول دیجیتال همین انتظار و یا حتی بیشتر از این را نداشته باشیم؟

1 Crypto proof
2 Equifax

برای حفظ ارزش پول باید به بانک‌های مرکزی اعتماد کنیم، اما سرگذشت پول‌های فیات پر از موارد نقض این اعتماد است

فیات[1] به لاتین یعنی «تعیین شده» و درواقع پولی است که دولت و بانک مرکزی منتشر می‌کنند و توسط دولت به عنوان پول قانونی تعیین می‌شود. در گذشته پول توسط افراد فعال بازار و 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 در سال ۱۹۷۱ توسط نیکسون[2] از هرگونه پشتوانه فیزیکی جدا شد و امکان تبدیل آن به طلا در همه جهان متوقف شد. با پایان پول‌طلا[3]، دولت‌ها و بانک‌های مرکزی اجازه پیدا کردند تا عرضه پول را به میل خود افزایش دهند. این امر باعث کاهش ارزش اسکناس‌های درگردش شد که تحت عنوان کاهش ارزش پول[4] 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 مفهوم نسبتاً جدیدی است که حدود یک قرن قدمت دارد.

ما به دولت‌های خود اعتماد می‌کنیم که از چاپخانه‌های پول خود سوءاستفاده نمی‌کنند ولی برای پیدا کردن بدعهدی‌های آنان نیازی نیست خیلی به گذشته برگردیم. در رژیم‌های استبدادی و با برنامه‌ریزی متمرکز سوسیالیستی مثل ونزوئلا که دولت انگشت خود را مستقیماً روی دستگاه چاپ پول می‌گذارد، پول تقریباً بی‌ارزش شده است. نرخ تبدیل بولیوار ونزوئلا از ۲ واحد در مقابل هر دلار در سال ۲۰۰۹ به ۲۵۰,۰۰۰ واحد در سال ۲۰۱۹ رسید. در زمان نگارش این کتاب ونزوئلا به دلیل سوء مدیریت سرمایه توسط دولت در مرحله سقوط و تغییر رژیم است.

1 Fiat
2 Nixon
3 Gold Standard
4 Debasement

برخلاف پول فیات که عرضه و ارزش آن قابل پیش‌بینی نیست، ساتوشی برای جلوگیری از کم ارزش شدن، نوعی سیستم پولی طراحی کرد که در آن حجم پول ثابت، از قبل مشخص شده، و غیرقابل تغییر است. نهایتا ۲۱ میلیون بیت‌کوین تولید خواهد شد و هر بیت‌کوین نیز می‌تواند به ۱۰۰ میلیون واحد تقسیم شود که به هر واحد آن ساتوشی[1] گفته می‌شود.

قبل از بیت‌کوین 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 می‌شوند مستثنی هستند و نمی‌توان آنها را کپی یا ارسال کرد. برای مثال وقتی فیلمی را از آیتونز[2] اجاره می‌کنید فقط و فقط در دستگاه شما قابل پخش است؛ چراکه آیتونز 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.

بیت‌کوین اولین شبکه دیجیتالی است که کمیابی دیجیتال را بدون نیاز به هرگونه واسطه‌ای پیاده کرده و تنها داراییِ شناخته‌شده برای انسان است که حجم آن غیرقابل تغییر 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 آن خواهیم پرداخت.

1 Satoshi
2 iTunes

داده‌ها می‌توانند به نحوی ایمن شوند که دسترسی فیزیکی به آن‌ها برای هیچکس ممکن نباشد [...] وقت آن فرا رسیده است پولی با چنین قابلیتی داشته باشیم

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

شاید برای فردی که در امریکا یا در یک اقتصاد قانونمند زندگی می‌کند از دست رفتن پول به این صورت احمقانه به نظر برسد. به عنوان مثال حساب من در پی‌پال به دلیل استفاده نکردن از آن بلوکه 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 پی‌پال پول من را بلوکه کند، می‌شود به یک مرجع قانونی مراجعه کرد و همینطور می‌توان به دولت و بانک اطمینان داشت که پول کسی را سرقت نمی‌کنند.

موارد بدتری در بعضی کشورها که از آزادی کمتری برخوردارند رخ داده است و همچنان رخ می‌دهد، مثل اینکه بانک‌ها در یونان هنگام سقوط ارزش پول ملی بسته شدند، یا اینکه بانک‌ها در قبرس با دزدی از مشتریان خود از وثیقه‌ها سوءاستفاده می‌کردند، یا دولت هند که اسکناس‌های مشخصی را بی‌ارزش اعلام کرد و باعث ایجاد صف‌های طولانی مقابل خودپردازهای بانک‌ها و درنهایت منجر به مرگ بعضی افراد صرفاً بخاطر عدم دسترسی به سرمایه‌شان شد.

شوروی سابق، جایی که من بزرگ شدم، دارای یک اقتصاد به‌شدت کنترل‌شده مرکزی بود که باعث کمبود کالاها می‌شد. 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، به دلار تبدیل کند.

بیت‌کوین سیستمی ایجاد کرده است که در آن برای تأمین امنیت پول نیازی به اعتماد به شخص سوم نیست. در این سیستم با استفاده از کلیدهای خاصی که تنها در اختیار شما قرار دارد از دسترسی دیگران به کوین‌های شما جلوگیری می‌شود. مهم نیست افراد مختلف چه دلایلی برای دسترسی به حساب شما دارند، در هر صورت دسترسی به دارایی شما فقط از طریق شما ممکن است.

بیت‌کوین پول را از دولت جدا می‌کند و موجب مهار قدرت خودکامه‌گان و دیکتاتورها می‌شود و حق در دست داشتن اختیار دارایی، و آزادی در نقل و انتقال آن ورای مرزهای جغرافیایی بدون دخالت هیچ فردی را به مردم بازمی‌گرداند.

راه حل بیت‌کوین برای جلوگیری از دوبار خرج کردن[1] استفاده از یک شبکه نظیر به نظیر است. به طور خلاصه این شبکه شبیه به یک سرور زمان‌سنج توزیع شده[2] کار می‌کند که اولین تراکنش را برای خرج کردنِ یک کوین(سکه) 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 کنترل‌کننده مرکزی، تمامی اعضای شبکه با هم در تعامل هستند تا شبکه را ایجاد کنند.

در یک سیستم بدون کنترل مرکزی، اطمینان از اینکه هیچ‌یک از اعضا تقلب نمی‌کنند حائز اهمیت است. اصطلاح «دوبار خرج کردن» به این معنا است که یک کوین توسط

1 Double Spend
2 Distributed timestamp server

یک فرد دوبار خرج شود. ساتوشی می‌گوید برای پیشگیری از این اتفاق، اعضای شبکه بیت‌کوین با هم همکاری می‌کنند تا تراکنش‌ها را برچسب زمانی بزنند (یعنی براساس زمان اعلام به شبکه 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 وابستگی به یک نهاد مرکزی، تراکنش‌های جعلی را شناسایی کند.

اختراع بیت‌کوین شماری از مشکلات مهمی که در سیستم‌های رایج مالی در زمینه حریم خصوصی، کاهش ارزش پول و کنترل مرکزی با آن‌ها دست به گریبان هستیم را حل کرده است. مشکلاتی از قبیل:

۱. چگونه یک شبکه نظیر به نظیر ایجاد کنیم که هرکس بتواند داوطلبانه به آن متصل و عضوی از آن شود.
۲. چگونه یک گروه از افراد که یکدیگر را نمی‌شناسند یا اعتمادی به هم ندارند می‌توانند اطلاعات ارزشمندی را با هم به اشتراک بگذارند؛ چراکه ممکن است بین آنها افراد متقلب نیز وجود داشته باشد.
۳. چطور بدون واسطه، یک کمیابی دیجیتالِ واقعی بسازیم.
۴. چگونه یک دارایی دیجیتال ایجاد کنیم که قابل جعل کردن نباشد، اصالت آن به‌صورت آنی تأیید شود، و در برابر هک و سرقت مقاوم باشد.

بیایید فکر کنیم چطور می‌توانیم چنین سیستمی بسازیم.

فصل دوم

حذف واسطه‌ها

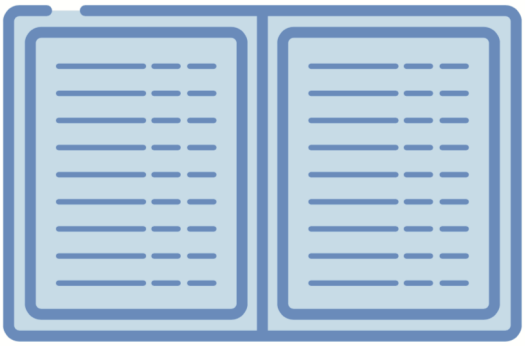
در فصل قبل گفته شد که بیت‌کوین یک سیستم نظیر به نظیر برای انتقال پول است. بیایید قبل از اینکه این مورد را بررسی کنیم، گذری بر نحوه عملکرد بانک‌های سنتی و سیستم‌های پرداخت در بررسی مالکیت و انتقال پول داشته باشیم.

بانک‌ها چیزی جز یک دفترکل حسابداری[1] نیستند

یک سیستم پرداخت که توسط بانک یا پی‌پال ویا اپل پِی ساخته شده است، چگونه کار می‌کند؟ خیلی ساده؛ این واسطه‌ها یک دفترکل حسابداری حاوی اطلاعات حساب‌ها و نقل و انتقالات آنها دارند.

در این مثال از لفظ بانک استفاده می‌شود ولی منظور هرنوع سیستم پرداخت است. با یک دفترکل حسابداری حاوی اطلاعات سپرده «آیدا» و «بابک» در بانک شروع می‌کنیم.

1 Ledger



دفتر کل بانک

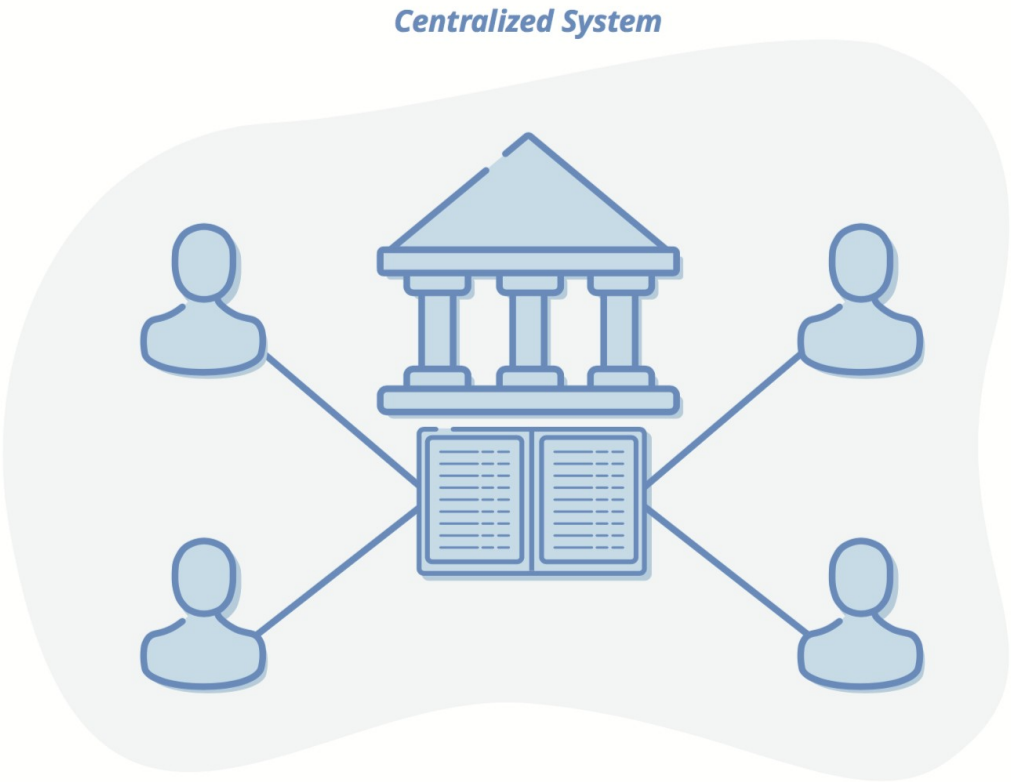
۱. آیدا: سپرده نقدی +۲۰هزارتومان
۲. بابک: سپرده نقدی +۱۰۰هزارتومان

وقتی آیدا می‌خواهد ۲۰ه.ت برای بابک بفرستد با بانک خود تماس می‌گیرد یا با استفاده از نام کاربری و رمز عبور به اینترنت بانک یا موبایل بانک خود وارد می‌شود و سپس درخواست این انتقال وجه را در سیستم بانک وارد می‌کند. بانک هم این درخواست را در دفتر کل حسابداری‌اش ثبت می‌کند.

دفتر کل بانک

۱. آیدا: سپرده نقدی ۲۰+ هزارتومان
۲. بابک: سپرده نقدی ۱۰۰+ هزارتومان
۳. آیدا: کسر موجودی ۲۰- هزارتومان
۴. بابک: افزایش موجودی ۲۰+ هزارتومان

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



سیستم متمرکز

مشکل دوبار خرج کردن

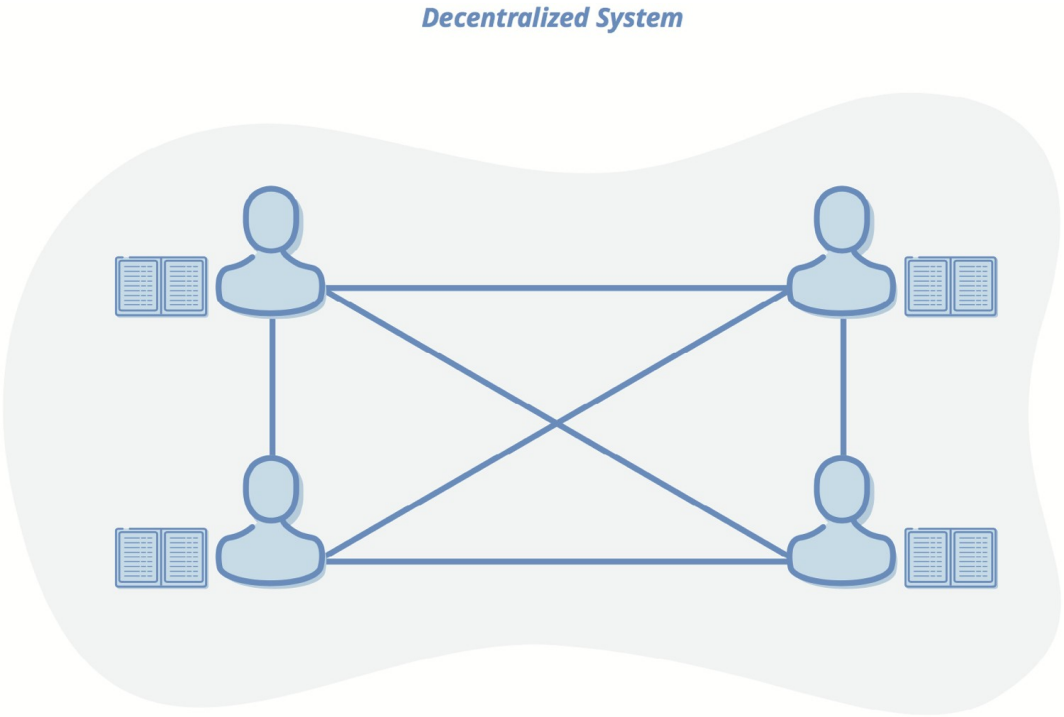
حال اگر آیدا بخواهد آن ۲۰ه.ت را دوباره خرج کند چه اتفاقی می‌افتد؟ به این اتفاق «دوبار خرج کردن» می‌گویند. آیدا درخواست خود را به بانک ارسال می‌کند، اما بانک می‌گوید: «شما قبلا ۲۰ه.ت خود را به حساب بابک واریز کرده‌اید و پولی ندارید.» وقتی یک مرجع مرکزی مثل بانک وجود دارد، برای بانک بسیار ساده است که بگوید 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 است و دستکاری نشده است. به چنین سیستم‌هایی متمرکز گفته می‌شود؛ چراکه فقط از یک نقطه کنترل می‌شوند.

بیایید دفترکل را غیرمتمرکز کنیم

اولین مشکلی که بیت‌کوین قصد حل آن را دارد حذف واسطه‌ی معتمد 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 از دفترکل نگهداری کرد؟

اگر دفترکل یک مسئول نداشته باشد، باید در اختیار همه قرار بگیرد. راه ایجاد یک دفترکل غیرمتمرکز هم همین 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 تلگرام هم را با یکدیگر ردوبدل می‌کنیم. وقتی آیدا قصد دارد پولی برای بابک ارسال کند، به‌جای تماس با بانک، در تلگرام به همه دوستان خود می‌گوید: «من ۲۰ه.ت به حساب بابک واریز می‌کنم.» همه تصدیق می‌کنند که این پیغام را دیده‌اند و پاسخ می‌دهند: «بله، ما پیغام را گرفتیم» و در دفتر کل‌ای که نزد خود دارند این جابه‌جایی را یادداشت می‌کنند. حالا سیستم به شکل زیر درخواهد آمد:



سیستم غیرمتمرکز

اکنون به‌جای اینکه فقط یک دفتر کل داشته باشیم و از آن در بانک نگهداری کنیم، یک نسخه 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 تلگرام اطلاع می‌دهد و یا با آن‌ها تماس می‌گیرد و آنها را مطلع می‌کند. همه افراد عضو شبکه این تراکنش را ثبت می‌کنند. این سیستم توزیع شده است چون دفتر کل در اختیار همه اعضای شبکه است و غیرمتمرکز است چون مسئولیت آن تنها بر عهده یک مرجع مرکزی نیست.

این سیستم چگونه مشکل دوبار خرج کردن را حل می‌کند؟ از آنجایی که همه افراد شبکه یک نسخه از دفتر کل حسابداری را نزد خود دارند، اگر آیدا بخواهد آن ۲۰ه.ت را که برای بابک ارسال کرده است دوباره خرج کند، این تراکنش توسط همه در شبکه رد می‌شود؛ چراکه هرکس دفتر کل خود را بررسی می‌کند و به آیدا 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 بین اعضایش را ثبت می‌کند. این سیستم بین گروهی از دوستانی که به دلایل اجتماعی رابطه نزدیکی با هم دارند و قصد تقلب ندارند، بسیار خوب عمل می‌کند، اما در مقیاس بزرگتر کارآمد نخواهد بود. هرچه تعداد اعضای این شبکه بیشتر شود، احتمال تقلب هم بیشتر خواهد بود.

چطور می‌توانیم جلوی بروز تقلب را بگیریم؟

فصل سوم

حذف اعتماد و حذف نیاز به کسب مجوز

تا زمانی که شبکه ما خصوصی باشد و هرکس برای پیوستن به دفتر حساب توزیع‌شده‌ای که پیشتر درباره آن صحبت کردیم نیازمند به اجازه گرفتن باشد و بنابراین ما بتوانیم به صداقت همه اعضا اعتماد کنیم، این سیستم به درستی عمل خواهد کرد. اما از این روش نمی‌توان برای میلیون‌ها نفر در سراسر جهان استفاده کرد.

سیستم‌های توزیع‌شده‌ای که هرکس می‌تواند در آن‌ها عضو شود، ذاتا قابل اعتماد نیستند. ممکن است بعضی از اعضاء به‌طور موقت به شبکه دسترسی نداشته باشند (آفلاین باشند)، و این یعنی آن‌ها در این مدت که به شبکه متصل نیستند از تراکنش‌هایی که در شبکه انجام می‌شود اطلاع نخواهند داشت. برخی دیگر ممکن است با تأیید یا ردِ وقوع یک تراکنش قصد تقلب داشته باشند. ممکن است افراد جدیدی به شبکه بپیوندند و نسخه‌های متناقضی از دفتر کل حسابداری را دریافت کنند. بیایید به روش تقلب در این سیستم نگاهی بیندازیم.

دوبار خرج کردن

اگر من آیدا باشم، می‌توانم با گروهی از اعضاء شبکه تبانی کنم و به آنها بگویم: «زمانی که من پولی را خرج می‌کنم آن را در دفتر خود ثبت نکنید؛ وانمود کنید که هرگز اتفاق

نیفتاده است». به این شکل آیدا می‌تواند پولش را دوبار خرج کند. آیدا با موجودی ۲۰ه.ت به این صورت عمل می‌کند:

۱. او ۲۰ه.ت از حساب خود برای خرید آب‌نبات به حساب بابک انتقال می‌دهد. حالا باید موجودی او صفر باشد.
۲. داوود و آوا و فرانک با آیدا تبانی کرده‌اند و تراکنش آیدا به بابک را در دفتر حسابداری خود ثبت نمی‌کنند. در نسخه‌ای که نزد آن‌ها است آیدا هرگز پولی به بابک پرداخت نکرده است.
۳. فرزین یک فرد قابل اعتماد است که یک نسخه از دفتر کل را دارد. او تراکنش آیدا به بابک را ثبت می‌کند و حالا در دفتر کل او موجودی آیدا صفر است.
۴. حمید یک هفته در تعطیلات بوده است و از هیچ‌یک از تراکنش‌ها اطلاعی ندارد. او به شبکه متصل می‌شود و تقاضای یک نسخه از دفتر حسابداری را می‌کند.
۵. حمید چهار نسخه نادرست از داوود و آوا و فرانک و آیدا، و یک نسخه صحیح از فرزین دریافت می‌کند. او چطور متوجه شود که کدام‌یک صحیح است؟ چون سیستم بهتری وجود ندارد، به آنچه که در اکثریت دفاتر وجود دارد اعتماد می‌کند و نسخه نادرست را به عنوان نسخه صحیح قبول می‌کند.
۶. آیدا با آن ۲۰ه.ت (که قبلاً خرج کرده) یک آب‌نبات از حمید می‌خرد. حمید این پول را از او می‌پذیرد چراکه براساس دانسته‌هایش آیدا هنوز ۲۰ه.ت در حساب خود دارد (براساس نسخه‌ای که از اکثریت گرفته است).
۷. حالا آیدا دو آب‌نبات دارد و ۴۰ه.ت پول جعلی در سیستم ایجاد کرده است. او از این آب‌نبات‌ها به دوستان خود می‌دهد و لطف آن‌ها را جبران می‌کند، و آن‌ها نیز این کار را صدها بار برای هرشخص جدیدی که به شبکه متصل می‌شود، تکرار می‌کنند.
۸. حالا آیدا صاحب همه آب‌نبات‌ها است و بقیه اعضاء پول‌های تقلبی دارند.
۹. افرادی که پول تقلبی از آیدا دریافت کرده‌اند، وقتی بخواهند آن را خرج کنند، آوا و فرانک و داوود که کنترل بیشتر شبکه را در اختیار دارند، این تراکنش را رد می‌کنند چون می‌دانند که پول اساساً جعلی است.

اینجا مشکل عدم توافق[1] بین اعضا بوجود می‌آید. افراد در یک شبکه درمورد نسخه صحیح دفتر کل حسابداری با یکدیگر توافق ندارند؛ چون چاره‌ای جز پیروی از رأی اکثریت نیست. درحالی‌که اکثریت افرادی که کنترل شبکه را دردست دارند متقلب هستند و پول‌های تقلبی که از هیچ خلق کرده‌اند را خرج می‌کنند.

اگر بخواهیم سیستمی راه بیندازیم که عضویت در آن نیاز به اعتماد و کسب اجازه نداشته باشد، باید طوری آن را طراحی کنیم که در برابر افراد سودجو و متقلب مقاوم باشد.

حل مشکل اجماعِ غیرمتمرکز[2]

حالا باید یکی از سخت‌ترین مسائل در علم کامپیوتر را حل کنیم: اجماع غیرمتمرکز بین افرادی که بعضی از آنها متقلب و غیرقابل اعتماد هستند. این مشکل تحت عنوان فرماندهان بیزانسی[3] شناخته می‌شود و اصلی‌ترین چیزی است که ساتوشی در اختراع بیت‌کوین از آن استفاده کرده است. بیایید این موضوع را بررسی کنیم.

ما باید سیستم را طوری پیاده کنیم که اعضای این شبکه روی موارد ثبت شده در دفتر کل حسابداری با هم به توافق برسند، بدون اینکه نیاز باشد بدانیم دارنده کدام دفتر کل تمام تراکنش‌ها را به درستی ثبت کرده است.

یک راه حل ساده‌لوحانه این است که یک فرد مورد اعتماد را برای نگهداری از دفتر کل تعیین کنیم. به‌جای اینکه همه‌ی اعضا تراکنش‌ها را ثبت کنند، تعداد انگشت‌شماری از دوستان مورد اعتماد مثل فرزین و کامبیز و فرانک و فیروزه را انتخاب کنیم تا تمام تراکنش‌ها را ثبت کنند چون می‌دانیم آن‌ها متقلب نیستند.

1 Consensus failure
2 Distributed Consensus Problem
3 Byzantine Generals

بنابراین هر زمانی که بخواهیم تراکنشی انجام دهیم به‌جای اطلاع‌رسانی به همه دوستان‌مان، فقط به فرزین و گروه منتخب او خبر می‌دهیم و آن‌ها هم در ازای دستمزد ناچیزی، دفتر کل را به‌روز و از آن نگهداری می‌کنند. بعد از اینکه آنها تراکنش را ثبت کردند با همه اعضایی که دفتر کل را به عنوان پشتیبان نگهداری می‌کنند، تماس می‌گیرند و ورودی‌های جدید دفتر کل را به اطلاع آن‌ها می‌رسانند.

این سیستم به خوبی کار می‌کند، تا روزی که ماموران دولتی وارد ماجرا می‌شوند و می‌خواهند بدانند چه کسانی این سیستم مالی را می‌گردانند. آن‌ها فرزین و گروه منتخب را دستگیر می‌کنند و این پایانی برای دفتر کل حسابداری غیرمتمرکز ما خواهد بود.
نسخه‌های پشتیبان نزد اعضای شبکه قابل اعتماد نیستند و به یکدیگر نیز نمی‌توانیم اعتماد کنیم. حتی نمی‌دانیم برای شروع دوباره این سیستم باید از نسخه پشتیبان چه کسی استفاده کنیم.

دولت می‌تواند به‌جای تعطیل و خاموش کردن این سیستم، افرادی که از دفتر کل نگهداری می‌کنند را در خفا تهدید به بازداشت کند و آن‌ها را مجبور کند تراکنش‌های آیدا (که مشکوک به فروش مواد مخدر است) را در شبکه نپذیرند و در دفتر کل حسابداری ثبت نکنند. در این صورت سیستم ما درواقع تحت کنترل مرکزی است و دیگر نمی‌توان آن را بی‌نیاز از مجوز خواند.

چطور است روش دموکراسی را امتحان کنیم؟ یک جمع ۵۰ نفره از افراد قابل اعتماد را مشخص می‌کنیم، و هر روز به‌صورت چرخشی انتخابات برگزار می‌شود که کدامیک از آن‌ها تراکنش‌ها را در دفتر حسابداری ثبت کند. هر عضو شبکه یک رای خواهد داشت. این سیستم تا زمانی که کار به خشونت و اعمال فشار مالی نکشد، خوب کار می‌کند. در غیر این صورت پایان مشابهی با روش‌های گذشته خواهد داشت:

۱. تهدید رای‌دهندگان برای انتخاب فرد مورد نظر دولت
۲. تهدید رای‌آورندگان برای ثبت تراکنش‌های جعلی در دفتر حسابداری

مشکل این است، وقتی اشخاص خاصی برای نگهداری از دفتر کل حسابداری تعیین می‌شوند، باید صادق و قابل اعتماد باشند و از طرف مقابل ما راهی برای دفاع دربرابر کسانی که آنها را مجبور به انجام کارهای نادرست می‌کنند، نداریم.

هویت جعلی و حمله سیبیل[1]

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

هروقت اعتماد بر پایه هویت افراد باشد ما خود را در معرض حمله سیبیل 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 دست برادرش بوده است؟ 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. بنابراین، بسیار با اهمیت است که در برابر تهدیدها از افرادی که از دفتر کل نگهداری می‌کنند، محافظت کنیم، اما چطور؟

1 Sybil attack

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. این سیستم باید به گونه‌ای باشد که هرکسی بتواند در آن عضو شود و رأی‌گیری در کار نباشد؛ چراکه در روش رای‌گیری مشکلات خرید رأی افراد و اعمال خشونت و تهدید برای تغییر رأی آنها وجود دارد.

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

۱. هرکسی در دنیا می‌تواند عضو سیستم باشد. ده‌ها هزار نفر می‌توانند به قرعه‌کشی نگه‌دارندگان دفتر کل در شبکه بپیوندند.
۲. زمانی که قصد ارسال پول داریم تمام شبکه را از این امر مطلع می‌کنیم، همان‌طور که قبلاً هم می‌کردیم.
۳. هر ۱۰ دقیقه یک برنده انتخاب می‌شود.
۴. زمانی که برنده انتخاب شد، آن شخص باید تمام تراکنش‌هایی را که اتفاق می‌افتد در دفتر کل ثبت کند.
۵. اگر شخص برنده فقط تراکنش‌های معتبر را در دفتر کل ثبت کند (سایر اعضا نیز باید اعتبار آن را تایید کنند) مبلغی به عنوان کارمزد به او تعلق می‌گیرد.
۶. هرکس یک نسخه از دفتر کل نزد خود دارد و اطلاعاتی که برنده قرعه‌کشی ارائه می‌دهد را به آن اضافه می‌کند.
۷. فاصله زمانی میان دو قرعه‌کشی ۱۰ دقیقه تعیین شده است تا مطمئن شویم افراد، زمان کافی برای به‌روزرسانی دفتر کل 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:

۱. چه کسی بلیت قرعه‌کشی را می‌فروشد و برنده را انتخاب می‌کند، درحالی‌که ما مشخص کرده‌ایم هیچ نوع مرجع مرکزی نباید وجود داشته باشد تا اجرای قرعه‌کشی به خطر نیفتد.
۲. چطور مطمئن شویم که برنده قرعه‌کشی واقعا تراکنش‌های درست را در دفتر کل ثبت کرده است و قصد تقلب 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 از اعتماد بی‌نیاز[1] باشد. باید سیستمی را ارائه دهیم که این ویژگی‌ها را داشته باشد:

۱. این امکان باید برای همه اعضاء (به‌طور یکسان) وجود داشته باشد که شخصا بلیت قرعه‌کشیِ خودشان را ایجاد کنند، چون به هیچ مرجعی نمی‌توان اعتماد کرد.
۲. بقیه اعضا باید به سادگی بتوانند با بررسی بلیت، صحت برنده شدن شما در قرعه‌کشی را تشخیص دهند، چون به کسی نمی‌توان برای تعیین برنده‌ی رقابت اعتماد کرد.
۳. اگر کسی برنده قرعه‌کشی شد و تراکنش نامعتبری را در دفتر کل ثبت کرد، باید راهی برای تنبیه او پیش‌بینی شود. به این صورت به‌جای اعتماد به افراد خاص در

1 Trustless

شبکه، با استفاده از مکانیزم‌های تشویقی و تنبیهی، اعتماد را در شبکه نهادینه می‌کنیم.

بیایید تک تک این موارد را حل کنیم. توضیح چگونگی انجام این قرعه‌کشی شاید سخت‌ترین چیز در فهمیدن بیت‌کوین باشد. برای همین، ۳ فصل بعدی را برای بررسی عمیق این مسئله درنظر گرفته‌ایم.

سیستم‌های استاندارد قرعه‌کشی مثل بخت‌آزمایی‌هایی که تحت نظارت یک مرجع مرکزی برگزار می‌شوند، توسط یک فرد اجرا می‌شوند. در این سیستم‌ها مجموعه‌ای از اعداد و تعدادی بلیت با شماره‌های تصادفی تولید می‌شوند. تنها یک بلیت شماره‌ای مشابه شماره محرمانه تولید شده توسط سازمان اداره‌کننده بخت‌آزمایی دارد. 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 یک قرعه‌کشی بخت‌آزمایی مسئولان از ترکیب اعداد برنده مطلع هستند. چون ما نمی‌توانیم چنین شخصی را در یک 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 هَش[1] برای این کار استفاده می‌کنیم. در فصل ۴ درباره آن مفصل صحبت خواهیم کرد.

درنهایت باید راهی برای تنبیه افراد متقلب داشته باشیم. تولید اعداد تصادفی، مثل بلیت بخت‌آزمایی، اساسا رایگان است. چطور این را به گونه‌ای ارائه دهیم که شما ملزم به پرداخت وجه برای خرید بلیت شوید درحالی‌که کسی وجود ندارد که از او بلیت بخرید؟

1 Hash

شما باید این بلیت را با هزینه کردن انرژی بخرید؛ منبع کمیابی که از هیچ به وجود نمی‌آید. در فصل ۵ این ایده شرح داده خواهد شد.

اثبات کار[1]: حل یک معمای دشوار و نامتقارن

راه حل مناسب برای این سه مشکل، به‌کار گرفتن روش اثباتِ کار است. این روش قبل از اختراع بیت‌کوین و در سال ۱۹۹۳ ابداع شده است.

قیمت بلیت قرعه‌کشی باید زیاد باشد وگرنه افراد، تعداد نامحدودی شماره بلیت 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 بیت‌کوین کردم و اینجا همان نقطه‌ای است که فیزیک در بیت‌کوین نقش ایفا می‌کند: قانون اول 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 آن را از هیچ به وجود آورید.

مفهوم اثباتِ کار بر این پایه 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.

1 Proof of Work

برای برنده‌شدن در قرعه‌کشی باید یک عدد خاص را تولید کنید که به لحاظ محاسباتی آن عدد از تراکنش‌هایی که قرار است در دفتر کل ثبت شوند 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 بلیت قرعه‌کشی خود را تولید کنند؛ با استفاده از یک سخت‌افزار یا نرم‌افزار و یک لیست از تراکنش‌هایی که باید در دفتر کل 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 تأیید آن دو مسأله را بررسی می‌کنند:

۱. عددی که شما تولید کرده‌اید از آستانه‌ای که همه درمورد آن توافق کرده‌اند کوچکتر است یا بزرگتر؟
۲. آیا این عدد از نظر ریاضی به راستی از مجموعه‌ای از تراکنش‌های معتبر که می‌خواهید در دفتر کل ثبت کنید به‌دست آمده است؟

این فرایند سیستم اثباتِ کار را به یک سیستم نامتقارن تبدیل می‌کند، به این معنا که تولید عدد بسیار سخت ولی اَعتبارسنجی آن آسان است.

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

برای مثال اگر تلاش کنید از پولی که قبلا خرج شده است دوباره استفاده کنید، بلیت 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 دفتر کل ثبت کنید، به عنوان پاداش بیت‌کوین دریافت خواهید کرد تا با آن هزینه انرژی صرف شده را پرداخت و کمی هم سود کنید.

ویژگی اثباتِ کار گران بودن آن است. بنابراین اگر کسی بخواهد از راه اعمال فشار و زور به اعضایِ این شبکه به آن حمله کند، صرف رفتن به خانه‌های آن‌ها کفایت نمی‌کند و گروه مهاجم باید هزینه‌های انرژی مصرف شده را هم بپردازد.

امروزه میزان انرژی مصرفی شبکه بیت‌کوین از مصرف برق برخی از کشورهای متوسط دنیا بیشتر تخمین زده می‌شود. پس برای تقلب در این شبکه نیاز به این مقدار انرژی برق خواهیم داشت.

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

فصل ۴

ریاضیات بیت‌کوین

قبل از اینکه درمورد چگونگی ارزیابی اثبات کار بحث کنیم، نیاز به اطلاعات مختصری از علم کامپیوتر داریم: بیت[1] و هش

هش کردن[2]

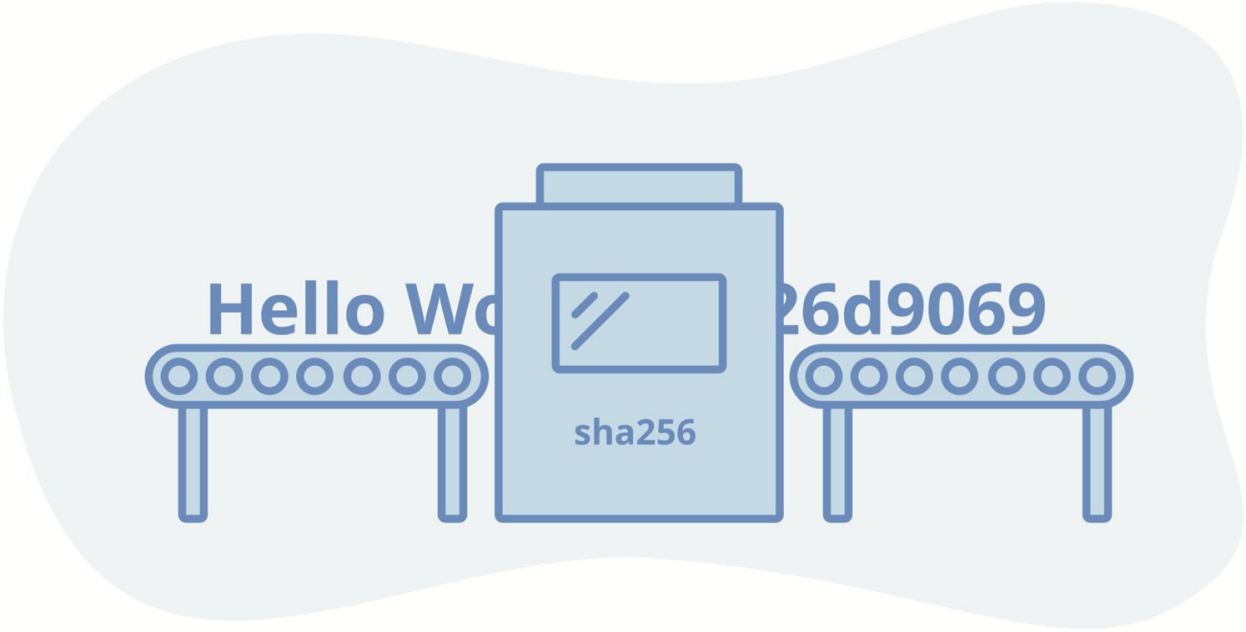
معمای نامتقارن اثباتِ کار در بیت‌کوین وابسته به استفاده از یک تابع هَش است. می‌دانیم که یک تابع مثل جعبه‌ای است که اگر مقدارX را به‌عنوان ورودی به آن بدهید، مقدار خروجیY را از آن دریافت می‌کنید. مثلا تابع f(x)=2x یک مقدار را می‌گیرد و در عدد ۲ ضرب می‌کند. اگر ورودی ۲ باشد خروجیِ تابع ۴ خواهد بود.

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. مثلاً برای رشته Hello world خروجی بلند زیر به‌دست خواهد آمد.

```
111181171325821924266132935775749045845
548904466436160011265843466335415020 95
```

1 bits
2 Hashing

من از تابع هشی به نام sha256 برای هش کردن Hello word استفاده کرده‌ام که در بیت‌کوین نیز استفاده می‌شود.



تابع sha256 ویژگی‌هایی دارد که برای ما مناسب است:

۱. خروجی آن قطعی است؛ یعنی برای یک ورودی ثابت همیشه یک خروجی ثابت دارد.
۲. خروجی آن غیرقابل پیش‌بینی است؛ یعنی 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.
۳. زمان محاسبه هش، صرف‌نظر از طول ورودی کوتاه است.
۴. اساساً غیرممکن است که دو رشته ورودیِ متفاوت، خروجی یکسانی داشته باشند.
۵. از خروجی تابع sha256 نمی‌توان ورودی را به‌دست آورد.
۶. اندازه خروجی همیشه ثابت است (در sha256 همیشه ۲۵۶ بیت است)

نگاهی کوتاه بر مفهوم بیت‌ها[1]

سیستم عددی که معمولاً از آن استفاده می‌کنیم شامل اعداد ۰ تا ۹ است که به آن سیستم دسیمال[2] (ده دهی) می‌گویند چون ۱۰ 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[3] (دو دویی) می‌گویند.

در سیستم دسیمال تنها از ارقام ۰ تا ۹ استفاده می‌شود. اگر بخواهید اعداد یک رقمی ایجاد کنید می‌توانید ۱۰ عدد مختلف داشته باشید از ۰ تا ۹. اگر بخواهید اعداد دورقمی ایجاد کنید می‌توان ۱۰×۱۰ عدد مختلف تولید کرد از ۰ تا ۹۹. برای سه رقم، ۱۰×۱۰×۱۰ عدد قابل تولید است از ۰ تا ۹۹۹.

تصور کنید که با N رقم چه عدد بزرگی را می‌توان تولید کرد. ۱۰ را N بار در خودش ضرب می‌کنیم، به عبارت دیگر ۱۰^N یا ۱۰ به توان N.

سیستم باینری هم به همین شکل کار می‌کند. تنها تفاوت آن تعداد ارقام قابل استفاده است. وقتی در سیستم دسیمال از ۱۰ 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 ۲ بیت می‌توان ۴ مقدار تولید کرد:۱۱،۱۰،۰۱،۰۰. شما می‌توانید این تعداد را از ضرب عدد ۲×۲ به‌دست آورید چون هر رقم می‌تواند دو مقدار مختلف داشته باشد.

1 Bits
2 decimal
3 binary

با ۳ بیت، $۲^۳ = ۲×۲×۲$ یعنی ۸ عدد مختلف می‌توان نشان داد: ۰۰۰، ۰۰۱، ۰۱۰، ۰۱۱،۱۰۰، ۱۰۱، ۱۱۱،۱۱۰.

پس با یک عدد باینری که طول آن N بیت باشد می‌توان ۲^N عدد مختلف ساخت.

بنابراین با یک عدد باینری ۲۵۶ بیتی، یعنی به اندازه خروجی تابع sha256، می‌توان $۲^{۲۵۶}$ عدد مختلف و غیرتکراری ایجاد کرد. این عدد به اندازه غیرقابل تصوری بزرگ است. در سیستم دسیمال، $۲^{۲۵۶}$ دارای ۷۸ رقم است، عددی به بزرگی تعداد اتم‌های کیهان[1].

$$2^{256} = 115,792,089,237,316,195,423,570,985,008,687,907,$$
$$853,269,984,665,640,564,039,457,584,007,913,129,639,936$$

این عدد، تعداد خروجی‌های ممکن با استفاده از تابع sha256 است. حدس زدن خروجی این تابع مثل پیش‌بینی ۲۵۶ بار پرتاب یک سکه پشت‌سرهم، یا پیش‌بینی مکان یک اتم خاص در جهان، تقریبا غیرممکن است.

به دلیل طولانی بودن این عدد، از این به بعد آن را به‌صورت $۲^{۲۵۶}$ نشان می‌دهیم که امیدوارم تصویر ذهنی درستی از احتمالات ممکن برای شما ایجاد کند.

بیایید یک رشته را هش کنیم

در اینجا تعدادی رشته حروف و هش sha256 آنها آورده شده است. خروجی آنها به شکل دسیمال نشان داده شده است اما در کامپیوتر این عدد به شکل رشته‌های باینری صفر و یک قرار می‌گیرد. می‌خواهیم ببینیم چطور با یک تغییر کوچک در ورودی، عدد

1 Universe

خروجی تغییر می‌کند و اینکه در تابع هش نمی‌توان براساس ورودی، خروجی را پیش‌بینی کرد:

```
“Hello world!”
52740724284578854442640185928423074974
81806529570658746454048816174655413720

“Hello world!!”
95863319874939535731602344194643497258 3
74513872780665335270495834770720452323
```

برای هیچ‌کس حتی کامپیوترها هم ممکن نیست بتوانند از خروجی تابع، رشته ورودی را پیدا کنند. اگر مایل باشید، در بعضی سایت‌ها امکان دیدن خروجی تابع هش sha256 به‌صورت آنلاین نیز وجود دارد و می‌توانید مقادیر دلخواه خود را در آن‌ها امتحان کنید.

هش کردن برای برنده شدن در قرعه‌کشی اثبات کار

بسیار خوب، دیگر الان می‌توانیم درباره موضوع اصلی صحبت کنیم. پیشتر گفتیم که $۲^{۲۵۶}$ خروجی ممکن برای تابع sha256 وجود دارد. اما فعلاً برای ساده‌تر شدن موضوع، بیایید فرض کنیم تنها ۱۰۰۰ خروجی ممکن برای تابع هش وجود دارد.

سیستم قرعه‌کشی به صورت زیر عمل می‌کند:

۱. آیدا اعلام می‌کند که می‌خواهد ۲۰ه.ت برای بابک ارسال کند.

۲. همه برای تراکنش «آیدا ۲۰ه.ت به بابک پرداخت می‌کند» در قرعه‌کشی شرکت می‌کنند و یک عدد تصادفی که به آن نانس[1] (عددی که فقط یک بار استفاده می‌شود) گفته می‌شود را 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.
۳. اگر عدد به‌دست‌آمده کوچکتر از عددی باشد که درباره آن توافق شده است (کمی جلوتر به آن خواهیم پرداخت)، برنده قرعه‌کشی مشخص می‌شود.
۴. اگر عدد به‌دست‌آمده بزرگتر از عددی باشد که روی آن توافق شده است (عدد هدف)، عملیات هش با یک عدد نانس متفاوت تکرار می‌شود:
«آیدا ۲۰ه.ت به بابک پرداخت می‌کند نانس=۱۲۳۴۵» سپس
«آیدا ۲۰ه.ت به بابک پرداخت می‌کند نانس=۹۲۳۴۵»، سپس
«آیدا ۲۰ه.ت به بابک پرداخت می‌کند نانس=۱۳۲۸۴۹۰۱۲۳۴۸۰۹۲۱»
و به همین ترتیب تا درنهایت عددی به‌دست 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 ۱۰۰۰ هش ممکن وجود داشته باشد و عدد هدف روی ۱۰۰ تعیین شده باشد، چه درصدی از هش‌ها کوچکتر از عدد هدف خواهند بود؟

در ۱۰۰۰ عدد ممکن بین صفر تا ۹۹۹، ۱۰۰ عدد وجود دارد که از ۱۰۰ کوچکتر هستند و ۹۰۰ عدد دیگَر بزرگتر. بنابراین ۱۰۰/۱۰۰۰ یا ۱۰٪ از هش‌ها کوچکتر از هدف هستند. درنتیجه اگر تمام رشته‌ها را هش کنید و تابع هش شما ۱۰۰۰ خروجی متفاوت داشته باشد، انتظار می‌رود که ۱۰٪ مواقع خروجی‌های شما کوچکتر از ۱۰۰ باشد.

سیستم قرعه‌کشی به این شکل کار می‌کند: یک عدد هدف مشخص می‌شود، و همه درمورد آن با هم به توافق می‌رسند (کمی جلوتر به آن خواهیم پرداخت که چطور این

1 Nonce (number used only once)

اتفاق می‌افتد). سپس همه تراکنش‌هایی که افراد به شبکه اعلام کرده‌اند را دریافت و آنها را هش می‌کنند و یک مقدار نانس 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 «آیدا ۲۰ه.ت به بابک پرداخت می‌کند، فرزین ۵۰ه.ت به آیدا پرداخت می‌کند» را دریافت کردم.
- مقدار نانس که مساوی با ۳۲۸۹۵ است را به انتهای آن اضافه کرده‌ام.
- به مقدار هش ۴۲ دست یافته‌ام که کمتر از هدف تعیین شده، یعنی ۱۰۰ است.
- این اثبات کار من است: داده‌های تراکنش، نانس‌ای که من اضافه کرده‌ام، و هش تولید شده براساس این ورودی‌ها.

ممکن است این موفقیت برای کسی که اثباتِ کار را به دست آورده، حاصل میلیاردها بار هش کردن برای رسیدن به خروجی مورد نظر و هزینه 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 خروجی به ورودی را ندارد اما محاسبه خروجی با فرض داشتن داده ورودی بسیار ساده و سریع است.

این فرایند چه ربطی به مصرف انرژی دارد؟ 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 معتبر خواهند بود. به این معنا 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.

فصل ۵

استخراج[1]

حالا آماده‌ایم تا ببینیم اثباتِ کار در بیت‌کوین واقعا چطور کار می‌کند:

۱. هرکس در هرجای دنیا می‌تواند با اتصال کامپیوتر خود به شبکه بیت‌کوین عضوی از آن باشد و تراکنش‌ها را دریافت کند.
۲. آیدا اعلام می‌کند که قصد دارد تعدادی کوین برای بابک ارسال کند. کامپیوترهای شبکه این تراکنش را بین هم پخش می‌کنند تا سراسر شبکه از آن مطلع شوند.
۳. همه کامپیوترهایی که قصد شرکت در این بخت‌آزمایی را دارند با اضافه کردن مقدار نانس و اجرای تابع sha256، شروع به هش کردن تراکنش دریافتی می‌کنند.
۴. اولین کامپیوتری که هشی را پیدا کند که کوچکتر از عدد هدف باشد برنده این بخت‌آزمایی است.
۵. این کامپیوتر، عدد برنده، همچنین مقدار ورودی (تراکنش و مقدار نانس) را اعلام می‌کند. این عمل ممکن است ساعت‌ها و یا فقط چنددقیقه طول بکشد. به تمام این اطلاعات درکنار هم (تراکنش، نانس، مقدار هشِ اثبات کار) یک بلاک[2] می‌گویند.
۶. بقیه اعضاء شبکه تراکنش‌ها و نانس بلاک ایجاد شده را بررسی می‌کنند تا مطمئن شوند مقدار هش به‌دست‌آمده واقعاً کوچکتر از مقدار هدف باشد و هیچ تراکنش

1 Mining
2 Block

نامعتبری در آن نیست. همچنین تاریخچه این بلاک نباید با بلاک‌های قبلی در تناقض باشد.

۷. همه اعضا این بلاک را در نسخه دفتر کل 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 دفتر را ایجاد کردیم. استخراج بیت‌کوین یعنی فرایند انجام عملیات اثباتِ کار، برنده شدن در آن، و نوشتن بلاک در دفتر کل بیت‌کوین.

بیت‌کوین‌های جدید چگونه استخراج می‌شوند؟

تا اینجا توضیح دادیم که آیدا چگونه ۲۰ه.ت برای بابک ارسال می‌کند. از این به بعد دیگر درباره تومان یا دلار صحبت نمی‌کنیم، چون بیت‌کوین چیزی از تومان یا ارزهای دیگر نمی‌داند. ما فقط بیت‌کوین داریم - یک واحد دیجیتال که بیانگر ارزش در شبکه بیت‌کوین است.

برای مرور مثالی پیشتر زدیم، آنچه دقیقا رخ داده این است که آیدا ۲ بیت‌کوین به حساب بابک ارسال می‌کند، درواقع بیت‌کوینی را که در حساب خودش ثبت شده بوده در حساب بابک ثبت می‌کند، و کسی که برنده قرعه‌کشی اثبات کار شود این تراکنش را در دفتر کل ثبت می‌کند.

اما آیدا آن دو بیت‌کوین را از کجا آورده است؟ بیت‌کوین چگونه شروع به کار کرد و چطور افراد قبل از اینکه جایی برای خرید بیت‌کوین وجود داشته باشد آن را به دست می‌آوردند؟

درواقع تولید بیت‌کوین یعنی مشارکت در فرآیند قرعه‌کشی و تلاش برای پیدا کردن اثبات کار و کسب اجازه برای نوشتن در دفتر کل. این فرآیند به استخراج معروف است. زمانی که شما با صرف میزان زیادی انرژی عدد نانسِ برنده قرعه‌کشی و بالتبع بلاک معتبری پیدا می‌کنید، اجازه دارید تراکنش‌هایی که از شبکه دریافت کرده‌اید را در آن ثبت کنید.

همچنین اجازه دارید علاوه بر تراکنش‌هایی که از شبکه دریافت کرده‌اید یک تراکنش بسیار خاص را هم به آن بلاک اضافه کنید، که به آن تراکنشِ کوین‌بِیس[1] می‌گویند. این تراکنش درواقع می‌گوید: «۱۲/۵ بیت‌کوین استخراج شد و به مریم که یک ماینر است بابت هزینه انرژی صرف شده برای پیدا کردن عدد اثبات کار و ساختن بلاک پرداخت می‌شود.»

پاداش استخراج بلاک

بنابر آنچه گفته شد، کسی که یک بلاک جدید استخراج می‌کند می‌تواند بیت‌کوین‌های جدیدی به حساب خود واریز کند. چرا این مقدار ۱۲/۵ است و ۱۰۰۰ نیست؟ چرا مریم نمی‌تواند تقلب کند و هرمقدار بیت‌کوینی که دوست دارد برای خود بردارد؟ این قسمت کلیدی است: بیت‌کوین یک سیستم بر پایه توافق توزیع‌شده[2] است. به این معنا که همه افراد باید درمورد آنچه که معتبر تشخیص داده شده است توافق داشته باشند.

اگر مریم یک بلاک را استخراج کند و بخواهد به خودش بیت‌کوین بیشتری پاداش دهد، این بلاک برای سایر اعضاء نامعتبر خواهد بود؛ چرا که در نرم افزار کاربران بیت‌کوین که همه آن را اجرا کرده‌اند کُدی وجود دارد که اعلام می‌کند: «جایزه این بلاک دقیقا ۱۲/۵ بیت‌کوین است. در صورت مشاهده بلاکی با مقداری بیشتر، آن را قبول نکنید.»

1 Coinbase
2 Distributed consensus

اگر مریم تقلب کند و بلاک نامعتبری ایجاد کند، آن بلاک در دفتر کلِ هیچ‌کس ثبت نخواهد شد و هزینه انرژی که او برای ساختن آن بلاک صرف کرده است به هدر می‌رود.

اولین بلاک توسط ساتوشی استخراج شده است. کُد بیت‌کوین 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 استخراج اولین بلاک عملیات اثبات کار و محاسبات لازم را انجام داده است.

در ابتدا جایزه استخراج هر بلاک ۵۰ بیت‌کوین بود، مقداری که ساتوشی برای استخراج اولین بلاک دریافت کرد. افراد دیگری هم که در همان روزهای اول به شبکه پیوستند به همین مقدار جایزه استخراج بلاک دریافت کردند.

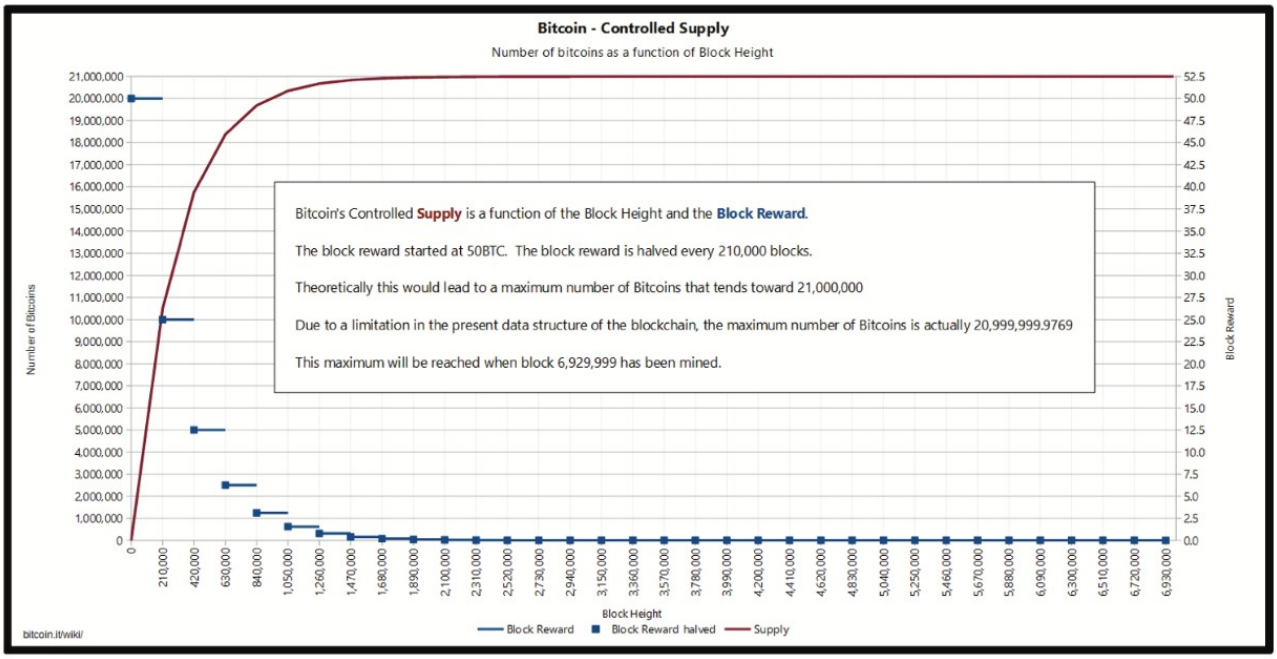
کُد بیت‌کوین هر چهارسال یک بار مقدار جایزه بلاک را نصف می‌کند (در اصطلاح رایج به این رویداد، هاوینگ[1] گفته می‌شود). این کاهش براساس تعداد بلاک‌های استخراج شده از ابتدای بیت‌کوین است، نه فقط گذر زمان، البته این دو موضوع تقریباً یکی هستند چون در هر ۱۰ دقیقه یک بلاک ساخته می‌شود.

در سال ۲۰۰۸ جایزه هر بلاک ۵۰ بیت‌کوین بود، در ۲۰۱۲ معادل ۲۵ بیت‌کوین و در سال ۲۰۱۶ معادل ۱۲/۵ بیت‌کوین. امروز، ۱۵ ژانویه ۲۰۱۹، تعداد ۵۵۸,۶۶۸ بلاک از ابتدای تاریخ بیت‌کوین استخراج شده است و جایزه آن ۱۲/۵ بیت‌کوین برای هر بلاک است.

۷۱,۳۱۲ بلاک دیگر، یا تقریباً حوالی ماه مه سال ۲۰۲۰ میلادی مقدار جایزه به ۶/۲۵ بیت‌کوین کاهش می‌یابد، که میزان عرضه بیت‌کوین را سالانه ۱/۸٪ افزایش خواهد داد. یک دهه بعد، که دوبار دیگر مقدار جایزه بیت‌کوین نصف شود، بیشتر از ۹۹٪ تمام

1 Halving

بیت‌کوین‌ها استخراج شده است و کمتر از ۱ بیت‌کوین برای تولید هر بلاک پرداخت خواهد شد.



https://en.bitcoin.it/w/images/en/4/42/Controlled_supply-supply_over_block_height.png

درنهایت در سال ۲۱۴۰ دیگر جایزه‌ای برای استخراج بلاک وجود نخواهد داشت و درآمد ماینرها از کارمزدی است که کاربران شبکه بیت‌کوین برای ارسال تراکنش‌ها به ماینرها پرداخت خواهند کرد.

قوانین خلق بیت‌کوین‌های جدید و تعداد جایزه بلاک‌ها در کُد بیت‌کوین تعیین شده است. تکرار می‌کنم که این کُد متن باز و بررسی برنامه تولید بیت‌کوین از راه پاداش بلاک برای همه امکان‌پذیر است. پس بلاکی که این قوانین را نقض کند از طرف همه کسانی که اجرای قوانین بیت‌کوین را از طریق اجرای کُد آن کنترل می‌کنند، رد خواهد شد.

کنترل فاصله زمانی استخراج بیت‌کوین‌های جدید

انجام عملیات استخراج به سخت‌افزار و برق نیاز دارد، بنابراین هرچه سخت‌افزار و برق بیشتری داشته باشید، به احتمال زیاد عدد برنده را سریع‌تر از سایرین پیدا خواهید کرد. برای مثال اگر ۱۰۰ کامپیوتر مشابه در شبکه وجود داشته باشد و ۱۰ تای آنها متعلق به شما باشد، در این صورت ۱۰٪ مواقع شما برنده خواهید بود. البته، فرایند استخراج براساس شانس و تصادف است و گاهی ممکن است ساعت‌ها یا حتی روزها هیچ بلاک جدیدی را نتوانید پیدا کنید.

با توجه به بخش‌های قبل می‌دانیم که ماینرها نمی‌توانند جایزه دلخواهی را برای خود تعیین کنند وگرنه بلاک آن‌ها توسط سایر نودهای شبکه رد می‌شود. اما اگر برای تسریع در ماین کردن بلاک‌ها انرژی بیشتری صرف کنند و بیشترین حجم استخراج بیت‌کوین در دست آنها باشد چه؟ در این صورت یکی از الزامات طراحی بیت‌کوین یعنی برنامه زمان‌بندی تولید بیت‌کوین‌های جدید زیر پا گذاشته خواهد شد.

بیایید به مثال برگردیم: تنها ۱۰۰۰ هش ممکن وجود دارد و عدد هدف ۱۰۰ است؛ به معنی اینکه در ۱۰٪ مواقع، عددی که تولید می‌شود کوچکتر از ۱۰۰ است و بلاک جدید پیدا می‌شود.

بیایید فرض کنیم زمان محاسبه هر هش یک ثانیه باشد. اگر هرثانیه یک بار تراکنش جاری را با عدد نانس هش کنیم و ۱۰٪ مواقع به عددی کوچکتر از عدد هدف برسیم، به طور میانگین ۱۰ ثانیه زمان برای پیدا کردن هش معتبر نیاز داریم.

حالا اگر دو کامپیوتر در این قرعه‌کشی شرکت کنند چه؟ سرعت دوبرابر می‌شود و انتظار می‌رود هر ۵ ثانیه هش معتبر پیدا شود. اگر با ۱۰ 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 به کار استخراج بیت‌کوین مشغول شوند، بلوک‌ها به سرعت ایجاد خواهند شد، که دو پیامد نامطلوب دارد:

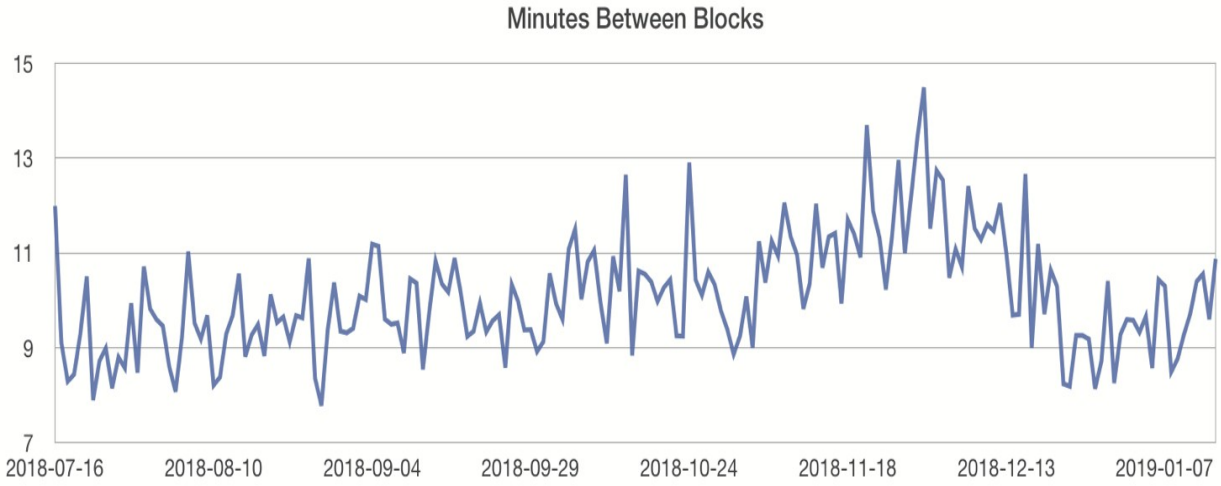
۱. در برنامه ازپیش تعیین‌شده‌ی عرضه بیت‌کوین اختلال بوجود می‌آورد. ما می‌خواهیم بیت‌کوین‌هایی که در هرساعت عرضه می‌شوند تعداد نسبتا ثابتی داشته باشند تا اطمینان حاصل شود که تا سال ۲۱۴۰ تمام بیت‌کوین‌ها عرضه شوند، نه زودتر.
۲. باعث ایجاد مشکل در شبکه می‌شود: اگر بلاک‌ها با سرعت بالایی استخراج شوند، زمان کافی وجود ندارد که بلاک به‌دست همه افراد شبکه برسد و قبل از اینکه همه از آن مطلع شوند بلاک ساخته شده است، بنابراین نمی‌توان درمورد تاریخچه بلاک‌ها به اجماع رسید. مثلا ممکن است که چند ماینر تراکنش یکسانی در بلاک خود داشته باشند و عملاً چون این تراکنش‌ها قبلاً در بلاک‌های قبلی خرج شده‌اند، این بلاکِ از نظر شبکه مردود باشد.

در مقابل اگر تعداد افراد کمتری به استخراج مشغول شوند این مشکلات پیش خواهد آمد:

۱. سرعت ساخت بلاک‌ها کم می‌شود و این موضوع باعث ایجاد اختلال در برنامه عرضه بیت‌کوین خواهد شد.
۲. اگر افراد مجبور باشند برای ثبت یک تراکنش در دفتر کل ساعت‌ها و روزها صبر کنند بلاک‌چین عملا غیرقابل استفاده خواهد بود.

به تعداد کل هشی که در هرثانیه توسط تمام ماینرهای شبکه بیت‌کوین انجام می‌شود «توان هش[1]» شبکه گفته می‌شود.

1 Hash Rate



زمان سپری شده بین استخراج بلاک‌ها

تنظیم سختی[1]؛ توافق روی 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 بیت‌کوین و زمان ساختن بلاک‌ها ثابت بماند؟

بیت‌کوین این مسئله را با تنظیم سختی استخراج[2] بلوک‌ها حل کرده است. از آنجایی که همه افراد شبکه کُد یکسانی را اجرا و بالتبع از قوانین مشترکی پیروی می‌کنند، و همه افراد یک نسخه از تاریخچه تمام بلوک‌ها تا آخرین آن‌ها را دارند، هرکسی می‌تواند به‌طور مستقل سرعت تولید بلوک‌ها را محاسبه کند.

در طول ۲ هفته باید ۲۰۱۶ بلاک ساخته شود، می‌توان بررسی کرد که تولید این تعداد بلاک چه‌قدر زمان برده است و سپس عدد هدف را برای بالا بردن یا کم کردن سرعت تولید بلاک‌ها تنظیم کرد.

1 Difficulty Adjustments
2 Mining difficulty adjustment

همه اعضای شبکه، ۲۰۱۶ بلاک آخر را دریافت کرده و بر زمان تولید آن تقسیم می‌کنند تا میانگین زمان تولید هر بلاک به‌دست آید. آیا بیشتر از ۱۰ دقیقه است؟ پس سرعت تولید هر بلاک 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 ۱۰ دقیقه فاصله زمانی که در کُد آمده است برسیم.

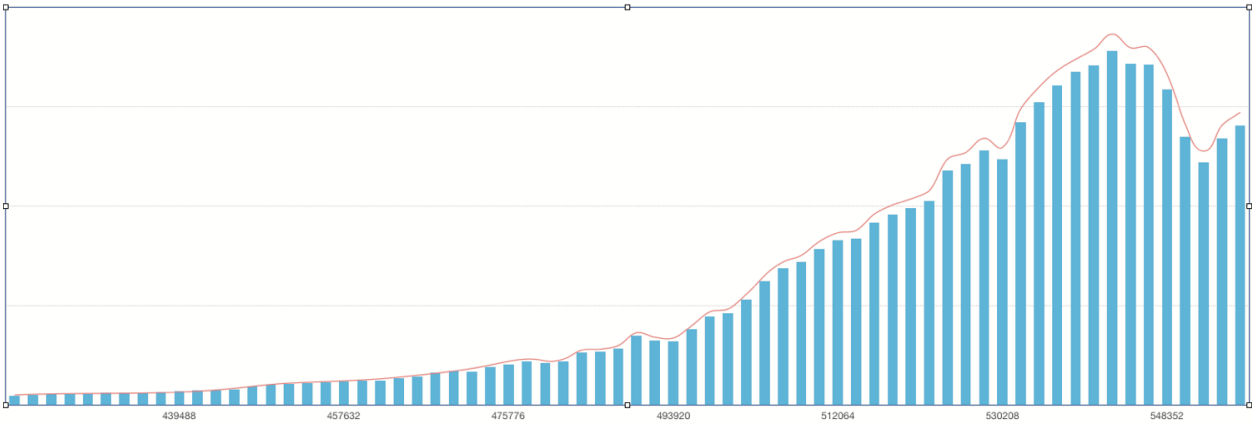
می‌توان عدد هدف را بزرگ‌تر انتخاب و بازه هش‌های معتبر را بیشتر کرد که در این صورت ماینرها شانس بیشتری برای برنده شدن خواهند داشت و انرژی کمتری هم مصرف می‌شود، که به آن کاهش سختی[1] می‌گویند. همچنین می‌توان عدد هدف را عدد کوچکی درنظر گرفت که در این صورت بازه هش‌های قابل قبول کوچک‌تر می‌شود و ماینرها باید انرژی بیشتری برای پیدا کردن هش معتبر هزینه کنند، که به آن افزایش سختی[2] گفته می‌شود.

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

با این روش هوشمندانه دیگر نیازی به یک مرجع مرکزی برای دریافت اطلاعات شبکه نداریم. تمام کاری که باید انجام دهیم این است که خودمان بررسی کنیم عدد هدف چه باشد و اینکه شماره بلیتی که ادعا می‌کند برنده بخت‌آزمایی است کوچکتر از عدد هدف است یا نه.

1 Lowering the difficulty
2 Raising the difficulty

نمودار زیر توان هشِ شبکه را به صورت یک خط، و سختی را به صورت میله‌ای نشان می‌دهد. نمودار سختی به شکل پله‌ای است چون با اضافه شدن هر ۲۰۱۶ بلاک، تنظیم می‌شود. می‌توان مشاهده کرد که هر زمان میزان توان هشِ شبکه بالاتر از سختی باشد، میزان سختی افزایش می‌یابد تا خود را به توان هشِ شبکه برساند. وقتی که توان هشِ شبکه کاهش پیدا می‌کند، همان‌طور که در اکتبر و دسامبر ۲۰۱۸ اتفاق افتاد، از سختی هم کاسته می‌شود. تنظیم سختی همیشه وابسته به میزان توان هشِ شبکه است.



مقایسه مقدار توان هش و سختی شبکه

به دلیل اینکه تنظیم سختی شبکه هر ۲۰۱۶ بلاک اتفاق می‌افتد، در فواصل این دوره‌های ۲۰۱۶ بلاکی ممکن است توان هشِ شبکه تغییرات ناگهانی داشته باشد و سرعت خلق بیت‌کوین‌های جدید سریع‌تر یا کندتر از برنامه زمان‌بندی پیش رود. درواقع در حال حاضر سرعت ما در مقایسه با برنامه‌ی عرضه تمام بیت‌کوین‌ها تا سال ۲۱۴۰، کمی بیشتر است. افزایش توان هشِ شبکه معمولاً به دلیل تولید سخت‌افزارهای جدیدی است که طی سال‌های اخیر ساخته شده است و با این‌حال تاثیر چندانی روی سرعت تولید بلاک‌ها در درازمدت نخواهد داشت و در آینده جبران خواهد شد.

تا اینجا تقریبا اختراع بیت‌کوین را کامل کرده‌ایم:

۱. جایگزین کردن بانک مرکزی با یک دفتر کل توزیع‌شده.
۲. ایجاد یک سیستم قرعه‌کشی برای انتخاب کسی که اجازه ثبت بلاک را در این دفتر کل دارد.
۳. با استفاده از سیستم اثباتِ کار، شرکت‌کنندگان قرعه‌کشی را به صرف انرژی برای خرید بلیت وادار کردیم و از طریق کنترل شماره هشِ تولید شده توسط شرکت‌کنندگان در این قرعه‌کشی، اعتبارسنجی بلیتِ برنده را برای همه اعضای شبکه آسان کردیم.
۴. به همه شرکت‌کنندگان در قرعه‌کشی اعلام شد که اگر برخلاف قوانین عمل کنند بلاک ساخته شده توسط آن‌ها رد خواهد شد و در نتیجه جایزه پاداش ساخت بلاک یا کوین‌بِیس به آنها پرداخت نخواهد شد. به این ترتیب یک روش اقتصادی برای جلوگیریِ از تقلب در شبکه ایجاد شد و همچنین انگیزه‌ای شد تا همه از قوانین پیروی کنند.
۵. محاسبه عدد هدف - بر اساس ۲۰۱۶ بلاک گذشته و قوانین کُد بیت‌کوین - را بر عهده شرکت‌کنندگان در قرعه‌کشی گذاشتیم و از این طریق زمان‌بندی تولید بیت‌کوین و تعیین عدد سختی را کنترل کردیم.
۶. برنامه زمان‌بندی عرضه بیت‌کوین را با استفاده از تنظیم سختی شبکه و تطابق آن با کاهش یا افزایش توان هشِ شبکه، اعمال کردیم.
۷. استفاده از کد متن باز برایِ اطمینان از اینکه همه می‌توانند صحت اجرای قوانین، اعتبارسنجی تراکنش‌ها، جایزه بلاک و محاسبه سختی را بررسی کنند.

هیچ مرجع مرکزی وجود ندارد. ما یک سیستم کاملا توزیع‌شده و غیرمتمرکز داریم. هرکسی می‌تواند به آن بپیوندد. هرکسی می‌تواند در قرعه‌کشی شرکت کرده و بیت‌کوین استخراج کند. همه می‌توانند از آن برای ارسال یا دریافت بیت‌کوین استفاده کنند. صحت

بلاک‌های تولید شده توسط کل شبکه احراز می‌شود و پاداش ساختن یک بلاک معتبر از طریق تراکنش کوین‌بیس به ماینرها تعلق می‌گیرد. ماینر یک بلاک نامعتبر تنبیه می‌شود و پاداش ساخت بلاک به او پرداخت نخواهد شد و ماینرها باید برای استخراج بلاک‌ها انرژی صرف کنند.

تقریبا تمام مطالب گفته شد، تنها یک مشکل باقی مانده است. زمانی که یک نفر به شبکه متصل می‌شود و یک نسخه از دفتر کل را درخواست می‌کند، ممکن است نسخه‌های متفاوتی از نودهای مختلف دریافت کند. چگونه یک تاریخچه یکپارچه و یکسان ایجاد کنیم و چگونه از بازنویسی مجدد دفتر کل توسط ماینرها جلوگیری کنیم؟

فصل ۶

ایمن کردن کوین‌ها در بلاک‌ها

تا اینجا درباره نحوه نگهداری از نسخه‌های دفتر کل و ثبت تراکنش‌ها در آن و از بین بردن امکان اعمال زور و تهدید و تقلب در طول این فرایند صحبت کردیم. اما اگر برنده قرعه‌کشی بخواهد خرابکاری کند چه؟ آیا فرد برنده می‌تواند تاریخچه بلاک‌ها را در تمام دفاتر کل دستکاری کند؟ آیا آوا و داوود و فرانک می‌توانند با هم تبانی کرده و تاریخچه بلاک‌ها را بازنویسی کنند، و یا موجودی حساب‌ها را تغییر دهند و کوین‌های اضافی به خود بدهند؟

از اینجا وارد بحث بلاک‌چین[1] می‌شویم. بلاک‌چین مفهومی است که در بسیاری از بخش‌های فناوری نفوذ کرده است. بلاک‌چین چیزی بیشتر از این نیست که بلاک‌های بیت‌کوین به هم وصل شوند تا مجموعه‌ای از تراکنش‌ها را به مجموعه بعدی متصل کنند.

در فصل‌های قبل برای ساده کردن موضوع کمی دروغ گفتیم. زمانی که اثباتِ کار را اجرا می‌کنید، اینطور نیست که فقط تراکنش‌هایی که قرار است در بلاک بعد نوشته شوند را به همراه مقدار نانس هش کنیم، بلکه هش بلاک قبلی هم به عنوان ورودی در تابع هش قرار می‌گیرد تا این بلاک را به بلاک قبلی متصل کند.

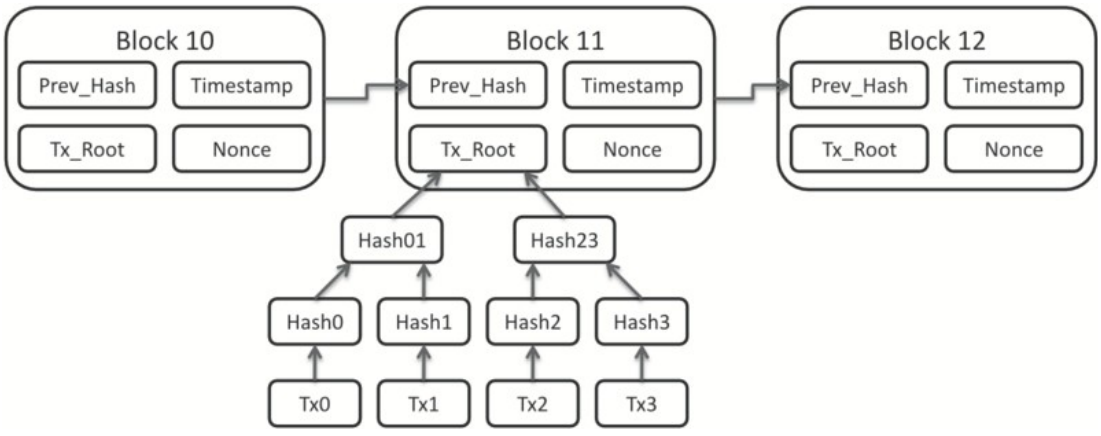
1 Blockchain

این کار باعث ایجاد یک تاریخچه برای هر بلاک می‌شود که به« اولین بلاک استخراج شده[1]» توسط ساتوشی برمی‌گردد. زمانی که یک بلاک در زنجیره نوشته می‌شود باید بررسی شود که تراکنش‌های موجود در آن با توجه به بلوک‌های 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:

۱. تراکنش‌هایی که باید در دفتر کل ثبت شوند
۲. مقدار نانس
۳. هش بلاک قبلی که به عنوان مبنایی برای تاریخچه دفتر کل از آن استفاده می‌کنیم

اگر یکی از این ۳ مورد تغییر کند، خروجی هش هم به شکل غیرقابل پیش‌بینی و به‌کلی 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.



https://upload.wikimedia.org/wikipedia/commons/7/7a/Bitcoin_Block_Data.png

1 Genesis Block

هرگونه تغییر در هریک از بلاک‌ها قابل تشخیص و دستکاری در آن کاملاً مشهود است[1]. 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 بیت‌کوین استخراج می‌شود، به امنیت بلاک‌های قبلی اضافه می‌کند. وقتی ۶ بلاک جدید بعد از ثبت یک تراکنش در دفتر کل ساخته شود، مثل این است که این تراکنش را روی سنگ حک کرده باشند و دیگر قابل تغییر نیست. چرا که برای بازتولید ۶ بلاک آخر، با توجه به توان هش‌ای که در حال حاضر در شبکه بیت‌کوین وجود دارد، مقدار زیادی انرژی باید صرف شود. اگر ۱۰۰ بلاک جدید بگذرد دیگر تغییر این تراکنش را به‌کل فراموش کنید.

مهم است که بدانیم هیچ قانونی برای تعیین نهایی شدن یک تراکنش در شبکه بیت‌کوین وجود ندارد. هر پرداخت‌ساز[2] یا فروشنده‌ای[3] خودش تصمیم می‌گیرد که با ساخته شدن چند بلاک جدید یک تراکنش را نهایی فرض می‌کند. امروزه اکثر افراد ۶ بار تایید تراکنش را (تولید ۶ بلاک بعد از بلاکی که تراکنش ما در آن است) به عنوان تایید نهایی آن درنظر می‌گیرند ولی این عدد برای هر کس ممکن است متفاوت باشد.

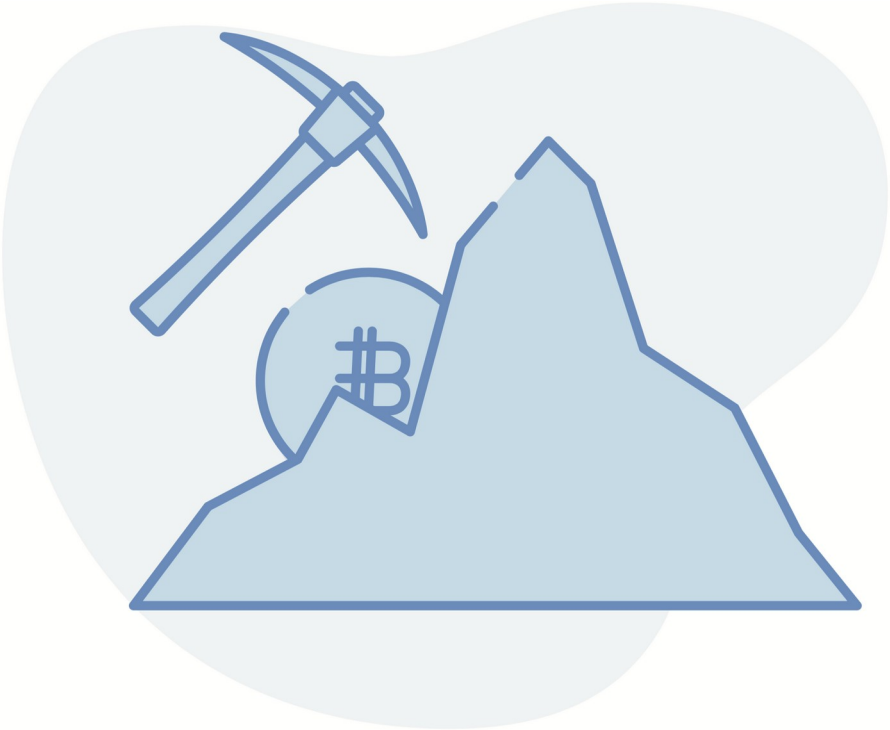
اگر شما کتاب دیجیتال که قیمت ناچیزی دارد می‌فروشید، ممکن است تنها یک تایید برای شما کافی باشد و یا حتی بدون هیچ تاییدی به محض اینکه تراکنش در شبکه پخش شد کالای دیجیتال را تحویل خریدار دهید. اگر بخواهید یک خانه را بفروشید ممکن است تا ۱۲ تایید که تقریبا ۲ ساعت طول می کشد، صبر کنید. هرچه بیشتر صبر کنید دفعات بیشتری عملیات اثباتِ کار انجام می‌شود و بلاک‌های بیشتری بعد از بلاکی که تراکنش شما در آن قرار دارد ایجاد می‌شوند و هزینه هرگونه تغییر در آن بلاک عملاً بیشتر می‌شود.

1 Tamper Evident
2 Payment processor
3 Merchant

اگر توان هش شبکه بیت‌کوین به اندازه قابل توجهی کاهش پیدا کند، به این معناست که مقدار انرژی کمتری امنیت بلاک را تضمین می‌کند، در این صورت افراد می‌توانند منتظر تعداد دفعات تأیید بیشتری بمانند و معامله را درصورت رسیدن به این تعداد دلخواه نهایی کنند. ممکن است این موضوع شما را کمی نگران کند ولی در نظر داشته باشید که تراکنش‌های کارت‌های اعتباری [در کشور ایالات متحده] ۱۲۰ روز بعد از انجام، قابل برگشت هستند. از طرف دیگر بیت‌کوین مثل طلا یا پول نقد است که کسی نمی‌تواند از چنگ شما دربیاورد. از نقطه‌نظر برگشت‌ناپذیری و نهایی بودن، تراکنش‌های بیت‌کوین در مقایسه با شبکه‌های پرداخت رایج سنتی خیلی پیشرفته‌تر است.

بیایید به مثال فصل ۳ برگردیم، جایی که حمید به شبکه متصل شد و نسخه‌های متفاوتی از دفتر کل دریافت کرد. دفتر کل‌ای که از فرزین دریافت کرد معتبر بود اما دفتر کل آوا و داوود و فرانک نادرست بود چون بلاکی که حاوی تراکنش آیدا بود را حذف کرده بودند و می‌توانستند حمید را گول بزنند که آیدا هنوز آن کوین‌ها را دارد. قبل از آنکه بلوک‌ها توسط اثباتِ کار به هم متصل شوند، حمید نمی‌توانست از حذف یک بلاک قدیمی (حاوی تراکنش آیدا) خبردار شود.

چون اثباتِ کار برای هر یک از بلوک‌ها محاسبه می‌شود، او براساس عددِ هدفِ تعیین شده در آنَ بلاک، می‌داند حدوداً چه مقدار انرژی برای تولید آن صرف شَده استَ. چون هر بلاک به بلاک قبلی خود متصل است، او می‌داند که با ایجاد تغییر در تراکنش‌های یک بلاک، اثباتِ کار نه‌تنها برای آن بلاک بلکه برای همه بلاک‌های بعد از آن نیز باید دوباره انجام شود. همچنین او تمام تراکنش‌های موجود در یک بلاک را می‌بیند و می‌تواند مطمئن شود که هیچ کوین‌ای دوبار خرج نشده است.



برخلاف استخراج طلا که آن هم نیاز به صرف انرژی دارد،
فرایند استخراج بیت‌کوین شبکه را در برابر دست‌کاریِ دفتر کل ایمن می‌کند

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

یک نکته از توافق در این سیستم باقی مانده است. تصور کنید که این شبکه در سراسر جهان درحال اجرا است. افراد در تمام دنیا از امریکا تا چین به این شبکه سراسری متصل شده‌اند و عملیات اثباتِ کار و قرعه‌کشی را انجام می‌دهند.

یک نفر در شیکاگو یک بلاک معتبر را پیدا و آن را در شبکه منتشر (اعلام) می‌کند و تمام کامپیوترهای واقع در ایالات متحده آمریکا این خبر را دریافت می‌کنند. در همین زمان یک‌نفر در شانگهای چین همان بلاک را چند ثانیه بعد از بلاکی که در شیکاگو پیدا شده بود، پیدا می‌کند. کامپیوترهای نزدیک به شبکه چین هنوز از بلاکی که در آمریکا پیدا شده است خبر ندارند و اول بلاکی که در کشور چین ساخته شده است را دریافت خواهند کرد.

با انتشار این دو بلاک توسط نودهای شبکه بیت‌کوین به یکدیگر دو نسخه از بلاک‌چین پدید می‌آید که با یکدیگر در رقابت‌اند. آمریکایی‌ها بلاک‌چینی دارند که بلاک آمریکایی در انتهای آن است و بلاک پیدا شده در چین هم به انتهای بلاک‌چین چینی‌ها وصل شده است. چون هردو بلاک‌چین مقدار اثباتِ کار یکسانی دارند و هردو حاوی تراکنش‌های معتبر هستند، شبکه به دو شاخه تقسیم می‌شود.

تعیین بلاک برنده در اختیار هیچ مرجعیت متمرکزی نیست. پس چه باید کرد؟ برای حل این مشکل، بیت‌کوین یک راه حل ساده دارد: باید صبر کنیم تا ببینیم چه پیش می‌آید. حالا دو نسخه از بلاک‌چین وجود دارد که در رقابت با هم هستند. حدودا ۱۰ دقیقه بعد بلاک بعدی ساخته خواهد شد. امریکایی‌ها براساس بلاک‌چین خود و چینی‌ها نیز براساس بلاک‌چین خود عملیات استخراج را انجام می‌دهند.

هرکدام که بتواند بلاک بعدی را پیدا کند برنده خواهد شد. چگونه؟ قانونی در کُد بیت‌کوین وجود دارد که می‌گوید در شرایطی که بلاک‌چین دوشاخه شود، زنجیره‌ای که طولانی‌تر است برنده خواهد بود. هرکس انرژی بیشتری را صرف کند برنده است؛ قانونی که ناهمخوانی بین زنجیره‌ها را براساس اثباتِ کارِ انباشته[1] آنها حل می‌کند و به افتخار ساتوشی ناکاموتو، اجماع ناکاموتو[2] نام‌گذاری شده است.

فرض می‌کنیم بلاک بعدی را چینی‌ها پیدا می‌کنند. حالا زنجیره آنها یک بلاک طولانی‌تر از زنجیره آمریکایی‌ها است. وقتی آن را در شبکه منتشر کنند نودهای بیت‌کوین آمریکایی متوجه می‌شوند که نودهای چینی زنجیره طولاتی‌تری را تولید کرده‌اند و بلاک‌چین خود را اصلاح[3] می‌کنند، یعنی بلاک خود را با دو بلاکی که چینی‌ها ساخته‌اند عوض می‌کنند. حالا به بلاکی که آمریکایی‌ها ایجاد کرده‌اند بلاک یتیم[4] می‌گویند؛ چراکه از طرف شبکه رد شده و استخراج‌کننده آن جایزه‌ای بابت آن نگرفته است.

1 Cumulative Proof of Work
2 Nakamoto Consensus
3 Reorg (Reorganization)
4 Orphan Block

اگرچه من از لفظ امریکایی و چینی برای اشاره به نودها استفاده کرده‌ام، اما در واقعیت آن‌ها از هویت و موقعیت جغرافیایی یکدیگر بی‌خبرند. تنها چیزی که باید بدانند این است که چه کسی طولانی‌ترین زنجیره از بلاک‌ها را دارد و تراکنش‌های موجود در زنجیره همگی معتبر هستند (هیچ کوین‌ای دوبار خرج نشده باشد و باقی قوانین).

احتمال دو شاخه شدن زنجیره بلاک‌چین بسیار کم است. در گذشته یک مورد در ماه و یا کمتر بود اما اخیرا به دلیل ارتقاء تکنولوژی انتشار بلاک‌ها و ارتباط بین استخراج‌کنندگان در شبکه این اتفاق تقریباً نادر است.

یکی از دلایلی که بیت‌کوین هر ۱۰ دقیقه بلاک‌های نسبتاً کوچکی (کمتر از ۲ مگابایت) تولید می‌کند برای این است که این بلاک‌های به اصطلاح یتیم تا جایی که ممکن است کمتر ایجاد شوند. دلیل دیگر، کاهش نیازهای سخت‌افزاری برای اجرای یک نود است تا افراد بیشتری تشویق به اجرای آن در سیستم شوند.

اگر در هرثانیه یک بلاک ساخته می‌شد یا اندازه بلاک‌ها خیلی بزرگ بود، مغایرت در زنجیره بلاک‌های چینی و آمریکایی با احتمال بیشتری رخ می‌داد، چون به لحاظ جغرافیایی فاصله زیادی با هم دارند و مدت زمان بیشتری طول می‌کشد تا اطلاعات بین آن‌ها منتقل شود. اگر ایجاد بلاک‌های به اصطلاح یتیم در شبکه زیاد باشد بلاک‌چین از بین خواهد رفت چون این بلاک‌های یتیم پشت‌سرهم تولید خواهند شد و نودهای شبکه دیگر نمی‌توانند روی تاریخچه یکپارچه تراکنش‌ها با هم به توافق برسند.

یک نود بیت‌کوین برای جلوگیری از حمله هکرهایی که ممکن است اطلاعات نادرستی به آن بدهند، فقط کافیست به یک نود متعبر که آخرین نسخه صحیح بلاک‌چین را در اختیار دارد، دسترسی داشته باشد. نودهای شبکه مدام با یکدیگر در ارتباط هستند و بلاک‌های تولید شده را با یکدیگر به اشتراک می‌گذارند. نود شما برای پیدا کردن صحیح‌ترین نسخه بلاک‌چین فقط کافیست بلاکچین‌ای که بیشترین اثباتِ کارِ انباشته را

در خود دارد، در شبکه پیدا کند. چون دیگران هم از این قانون که در کُد نرم‌افزار نوشته شده است پیروی می‌کنند، این اطمینان حاصل می‌شود که همه نودهای شبکه روی صحیح‌ترین نسخه دفتر کل با یکدیگر به توافق می‌رسند.

بنابراین ارسال یک نسخه ناصحیح از بلاک‌چین به یک نود برای هکرها کار دشواری است، چون برای رسیدن به هدف خود باید ارتباط آن نود به همه نودهای معتبر دیگر را قطع کنند و او را تنها به نودهای نامعتبر وصل کنند.

اگرچه انشعاب‌های(چند شاخه شدن) زنجیره بلاک‌چین در شبکه بیت‌کوین عمدتا تصادفی و به دلیل تأخیر در انتشار بلاک‌ها ایجاد می‌شوند، اما این احتمال نیز وجود دارد که یک عنصر مخرب بخواهد کنترل بلاک بعدی و محتوای تراکنش‌های آن را دردست بگیرد و از اجماع ناکاموتو سوء استفاده کند. این کار درصورتی ممکن است که فرد خرابکار کنترل بیش از ۵۰٪ توان هش شبکه را در اختیار بگیرد و طولانی‌ترین زنجیره را بر اساس بیشترین اثباتِ کارِ انباشته ایجاد کند. این مشکل به «حمله ۵۱٪[1]» معروف است که در فصل ۹ به‌طورِ مفصل درباره آن صحبت می‌کنیم.

امنیت و ارزش دلاری بیت‌کوین

گفته شد که شبکه بیت‌کوین عدد سختی تولید بلاک را براساس تعداد شرکت‌کنندگانی که در قرعه‌کشی شرکت می‌کنند (ماینرهایی که برای انجام هَش انرژی صرف می‌کنند) تنظیم می‌کند. اینجا همان نقطه‌ای‌ست که دنیای واقعی، دنیای دیجیتال را لمس می‌کند؛ قیمت بیت‌کوین، قیمت سخت‌افزار، قیمت انرژی، و مقدار عدد سختی رابطه پیچیده‌ای را ایجاد می‌کنند:

1 51% attack

۱. ماینرها برای تأمین انرژی استخراج و تولید بیت‌کوین هزینه می‌کنند چون فکر می‌کنند چیز باارزشی است.
۲. معامله‌گران، بیت‌کوین می‌خرند چون فکر می‌کنند قیمت آن تا x دلار افزایش می‌یابد.
۳. ماینرها x دلار برای تامین انرژی و سخت‌افزار استخراج بیت‌کوین هزینه می‌کنند.
۴. تقاضای بالای خریداران و افزایش قیمت بیت‌کوین، ماینرهای بیشتری را به سمت استخراج بیت‌کوین سوق می‌دهد.
۵. هرچه تعداد ماینرها بیشتر شود، یعنی انرژی بیشتری در شبکه بیت‌کوین صرف می‌شود و به امنیت بیشتر شبکه می‌انجامد. این امنیتِ بیشتر به خریداران اطمینان خاطر بیشتری می‌دهد و گاهی اوقات منجر به افزایش قیمت بیت‌کوین می‌شود.
۶. بعد از تولید ۲۰۱۶ بلاک، درنتیجه حضور ماینرهای بیشتر و بالا رفتن توان هشِ شبکه، عدد سختی تنظیم و تولید بلاک‌ها دشوارتر می‌شود.
۷. سختی بالاتر به معنای کوچکتر شدن عدد هدف است پس ماینرها بلاک‌های کمتری استخراج می‌کنند که باعث می‌شود برخی از آن‌ها بیشتر از x دلار برای عملیات استخراج بیت‌کوین هزینه کنند.
۸. بعضی از ماینرها دیگر هیچ سودی نمی‌کنند چون هزینه صرف شده برای انرژی استخراج بلاک‌ها از ارزش بیت‌کوین‌های به‌دست آمده بیشتر شده است. در این حالت بعضی ماینرها کار را متوقف می‌کنند.
۹. ۲۰۱۶ بلاک دیگر تولید می‌شود، سختی شبکه مجددا محاسبه می‌شود و این بار چون بعضی از ماینرها دستگاه‌های خود را خاموش کرده‌اند، سختی کاهش می‌یابد و درنتیجه تولید بلاک‌ها ساده‌تر می‌شود.
۱۰. سختی کمتر یعنی ماینرهایی که در دوره قبلی سود نمی‌کردند می‌توانند دوباره به شبکه برگردند و به استخراج مشغول شوند. یا ماینرهای جدیدی وارد بازی شوند.
۱۱. برو به مرحله ۱.

در یک بازار نزولی، با فروش بیش از حد کوین‌ها از سمت کاربران، این چرخه می‌تواند در جهت دیگری حرکت کند و باعث کاهش قیمت بیت‌کوین شود (اصطلاحاً دامپ اتفاق بیفتد) و ماینرها نتوانند سود کنند. با این وجود، برخلاف آنچه که در رسانه‌ها تحت عنوان مارپیچ مرگ[1] مطرح می‌شود، الگوریتم تنظیم سختی شبکه این اطمینان را حاصل می‌کند که همواره نوعی تعادل بین قیمت بیت‌کوین و تعداد ماینرها در شبکه وجود خواهد داشت، همچنین ماینرهای ناکارآمد را به نفع ماینرهایی که با ارزان‌ترین انرژی ممکن کار می‌کنند، کنار می‌زند.

در عمل در این چندسال گذشته، قیمت بیت‌کوین رشد سریعی داشته است همان‌طور که توان هش شبکه افزایش داشته است. هرچه توان هش شبکه بالاتر باشد، حمله به آن هم 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 بیت‌کوین تقریبا برابر با انرژی مصرف شده در یک کشور متوسط است.

1 Death Spiral

فصل ۷

حساب‌های بی‌نام

تا اینجا یک دفتر کل توزیع‌شده بدون نیاز به یک مرجع مرکزی، یک سیستم قرعه‌کشی برای انتخاب فردی که در آن بنویسد، یک سیستم پاداش برای ماینرهای خوب و تنبیه بدها، راهی برای تنظیم سختی شبکه تا مطمئن باشیم برنامه عرضه بیت‌کوین ثابت است، و در نهایت 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 از طریق ارائه مدارک هویتی به صورت حضوری، یا ارائه نام کاربری و کلمه عبور در اپلیکیشن‌های نِت بانک، اقدام به جابه‌جا کردن پول می‌کنید. بانک از این روش اطمینان حاصل می‌کند که یک شناسه هویتی بین دو نفر به اشتراک گذاشته نمی‌شود.

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

ایجاد یک «حساب بیت‌کوین[1]»

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

چه می‌شود اگر هرکس نام کاربری و کلمه عبور خودش را مدیریت 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 در اختیار داشته باشد. پس به چیزی قوی‌تر، بزرگتر و خاص‌تر از یک نام کاربری و کلمه عبور نیاز داریم. این شیوه با توجه به فصل‌های قبلی باید برای شما آشنا باشد؛ دوباره نیاز به یک عدد تصادفی بزرگ داریم.

همان‌طور که خرید بلیت بخت‌آزمایی با تولید شماره‌های تصادفی ممکن شد، از همین روش برای ایجاد حساب‌ها نیز استفاده می‌کنیم. برای ایجاد یک «حساب بیت‌کوین» که به آن آدرس می‌گویند، ابتدا یک جفت عدد ۲۵۶ بیتی تولید می‌کنیم که از لحاظ ریاضی با هم مرتبط هستند، به نام کلیدهای عمومی و خصوصی[2]. $۲^{۲۵۶}$ جفت کلید، عددی بسیار بزرگ و به اندازه اتم‌های موجود در کیهان است. بنابراین احتمال اینکه دو نفر جفت کلیدهای مشابهی تولید کنند تقریباً غیرممکن است.

این جفت کلید ویژگی‌های قابل توجهی دارند. می‌توان از آن‌ها هم برای رمزنگاری و هم برای رمزگشایی یک پیغام استفاده کرد. علاوه بر این 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.

1 Bitcoin Account
2 Public/Private key pair

بیایید ببینیم آیدا چطور برای بابک کوین ارسال می‌کند. برای دریافتِ یک تراکنش، بابک 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 بابک این شماره آدرس را با آیدا به اشتراک می‌گذارد، حالا آیدا می‌تواند برای بابک کوین ارسال کند.

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

این اثبات با استفاده از امضای دیجیتال[1] انجام می‌شود. آیدا یک تراکنش ایجاد می‌کند، که در اصل یک داده کامپیوتری است. چیزی شبیه به «آدرس ۱۲۳۴۵ مقدار ۲ بیت‌کوین برای آدرس ۵۶۷۸ ارسال می‌کند» با این تفاوت که شماره آدرس‌ها عدد بزرگی هستند. سپس آیدا تراکنش خود را هش کرده و با کلید خصوصی خود هش را رمزنگاری و یک امضای دیجیتال ایجاد می‌کند.

وقتی آیدا تراکنش خود را در شبکه منتشر می‌کند، کلید عمومی و امضای دیجیتال خود را هم به شبکه اعلام می‌کند. چون همه کلید عمومی آیدا را دارند می‌توانند امضای دیجیتال تراکنش را رمزگشایی کنند. اما نتیجه این رمزگشایی زمانی موفقیت‌آمیز خواهد بود که تراکنش واقعاً با کلید خصوصی که فقط در اختیار آیدا است، رمزنگاری شده باشد.

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

1 Digital Signature

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

برخلاف امضای چک یا رمز بانکی شما، امضای دیجیتال شما مختصِ داده‌های تراکنشی است که هربار ساخته می‌شود. از این جهت امکان دزدی یا استفاده آن‌ها در تراکنش‌های دیگر وجود نخواهد داشت. هر تراکنش امضای متفاوتی دارد حتی اگر براساس کلید خصوصی یکسانی تولید شده باشد.

آیا می‌توان یک کلید خصوصی را حدس زد؟

بیایید احتمال حدس زدن یک کلید خصوصی را بررسی کنیم. هر کس کلید خصوصی را در اختیار داشته باشد می‌تواند کوین‌هایی که در آدرس عمومی آن ذخیره شده است را جابجا کند. یادآوری می‌کنم که یک کلید از حداکثر ۲۵۶ بیت ساخته می‌شود. هر بیت تنها دو مقدار می‌تواند بگیرد (صفر و یک). می‌توانید هر بیت را مثل یک بازی شیر یا خط در نظر بگیرید.

اگر کلیدهای خصوصی ما ۱ بیتی بودند، حکم یک سکه دو رو را داشتند، یا شیر یا خط. از دو بار پرتاب یک سکه، حدس شما یک بار درست از آب در می‌آید.

مرور مختصری بر احتمالات به زبان ساده: احتمال وقوع چند رویداد با ضرب کردن احتمال رخ دادن تک‌تک آن‌ها محاسبه می‌شود. اگر در پرتاب سکه احتمال شیر آمدن ۱/۲ باشد، بنابراین احتمال شیر آمدن در دوبار پرتاب سکه برابر با ۱/۴ یا یک به ۴ خواهد بود.

اگر ۲ بیت داشته باشیم، مثل دوبار پرتاب سکه است. $۴=۲^۲$، بنابراین شانس شما ۱ به ۴ است.

نتیجه پرتاب ۸ بار پشت سر هم سکه، $۲^۸$ است یا ۱ به ۲۵۶.

یک پلاک شهربانی در ایالات متحده دارای ۶ رقم یا حرف است. تعداد حروف الفبای انگلیسی ۲۶ و تعداد ارقام موجود ۱۰ تا است، بنابراین جمعا ۳۶ کاراکتر برای پلاک وجود دارد. چون پلاک ۶ رقمی است تعداد پلاک‌هایی که می‌توان ایجاد کرد $۳۶^۶$خواهد بود. پس احتمال حدس زدن پلاک ۱ به ۲,۱۷۶,۷۸۲,۳۳۶ است.

یک کارت اعتباری ۱۶ رقم دارد. هر رقم می‌تواند ۱۰ مقدار داشته باشد. پس احتمال حدس زدن شماره کارت اعتباری $۱۰^{۱۶}$ است، یعنی یک به ۱۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰.
حدود $۱۰^{۵۰}$ اتم بر روی سیاره زمین وجود دارد. اگر به طور تصادفی یکی از اتم‌ها را درنظر بگیریم، شانس شما در حدس زدن آن چیزی حدود ۱ به

```
1,000,000,000,000,000,000,000,000,000,
000,000,000,000,000,000,000,000,000,000
```

یک کلید خصوصی ۲۵۶ بیت دارد، یعنی $۲^{۲۵۶}$ یا حدود $۱۰^{۷۷}$. درواقع عددی به بزرگی حدس زدن یک اتم خاص از کل هستی و یا ۹ بار برنده شدن پشت سر هم در بخت‌آزمایی. شانس شما در حدس زدن آن ۱ به

```
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 در اختیار داشته باشیم چه؟ این موضوع در یکی از پست‌های سایت ردیت[1] به خوبی توضیح داده شده است و پیشنهاد می‌کنم آن مطلب[2] را بخوانید. با وجود اینکه متن تخصصی است اما پاراگراف آخر آن می‌تواند تصور خوبی از فهرست کردن تمام کلیدهای ۲۵۶ بیتی ممکن را به شما بدهد:

> «اگر بتوانید از سیاره زمین به‌عنوان حافظه استفاده کنید، به ازای هر اتم یک بایت ذخیره کنید، از ستاره‌ها به عنوان سوخت استفاده کنید، و یک تریلیون کلید در ثانیه تولید کنید، نیاز به ۳۷ اکتیلیون[3] زمین برای ذخیره آن و ۲۳۷ میلیارد خورشید برای تامین انرژی سخت‌افزارها نیاز دارید و تمام این فرایند ۳/۶۷۱۷ اکتادسیلیون[4] سال طول خواهد کشید.»

– U/PSBLAKE on R/BITCOIN

1 Reddit
2 reddit.com/r/Bitcoin/comments/1rurll/on_the_subject_of_listing_all_possible_private
3 Octillion ($1x10^{27}$)
4 Octodecillion ($1x10^{801}$)

اساسا حدس زدن کلید خصوصی دیگران غیرممکن است. نه فقط این، بلکه تعداد آدرس‌های بیت‌کوین 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 بیت‌کوین داشته باشید؛ یک حساب جداگانه برای هر بار دریافت بیت‌کوین.

ممکن است این موضوع که امنیت حساب بیت‌کوین شما براساس شانس تامین می‌شود برای شما کمی نگران‌کننده باشد، اما امیدوارم نوشته بالا این اطمینان را به شما بدهد که امنیت این حساب بسیار بیشتر از رمز عبور حساب بانکی شماست که در یک سرور مرکزی ذخیره شده و در دسترس هَکرهاست.

بررسی موجودی حساب

حالا زمان تصحیح آخرین دروغ مصلحتی‌ای است که درباره نحوه کار بیت‌کوین گفتم. مانده حساب‌ها در دفترکل ثبت نمی‌شوند، به‌جای آن بیت‌کوین از یک مدل به نام «خروجیِ خرج‌نشده[1]» استفاده می‌کند. (با توجه به رایج بودن اصطلاح UTXO بین کاربران فارسی‌زبان، در ادامه از عبارت انگلیسی آن استفاده می‌کنیم. - م)
ایده UTXO به این صورت است که، هر تراکنش مجموعه‌ای از ورودی‌هایی است که برای تولید خروجی‌های جدید از آن‌ها استفاده می‌شود. مثل این است که تعدادی سکه فلزی را به یک دستگاه بدهیم تا آنها را ذوب کند و سکه‌های جدیدی و به هر اندازه‌ای که می‌خواهیم برای ما ضرب کند و به ما برگرداند. به بیان ساده UTXO، یک خروجی از تراکنش‌های قبلی است که هنوز به آدرس دیگری ارسال نشده یا به عبارت دیگر هنوز خرج نشده است. تراکنشِ پاداش تولید بلاک به ماینرها (کوین‌بِیس) هم تا وقتی خرج نشود یک UTXO محسوب می‌شود.

1 UTXO (Unspent Transaction Output)

به عنوان مثال، آیدا آدرسی دارد که ۱ بیت‌کوین در آن است. او می‌خواهد ۰/۳ بیت‌کوین برای بابک ارسال کند. او یک تراکنش ایجاد می‌کند که ورودی آن یک UTXO با ۱ بیت‌کوین است و دو خروجی به شرح: یک UTXO جدید به ارزش ۰/۳ بیت‌کوین به عنوان خروجی به آدرس بابک، و یک UTXO جدید دیگر به ارزش ۰/۷ بیت‌کوین به عنوان خروجی برای بازگرداندن باقیمانده به آدرس آیدا. باقی بیت‌کوین آیدا می‌تواند به همان آدرسی بازگردد که او تراکنش را از آن ارسال می‌کند، ولی برای رعایت حریم خصوصی بهتر است در حین ایجاد تراکنش یک آدرس جدید بسازد و باقیمانده را به آن ارسال کند.

از آنجا که در زنجیره بلوک‌ها راهی برای شناسایی صاحب یک آدرس وجود ندارد، (برای این منظور باید کلیدهای خصوصی هر آدرس بیت‌کوین را بدانید و آن‌ها را به هویت افراد در دنیای واقعی ارتباط دهید)، مدل UTXO با فراهم آوردن امکانِ ایجاد و به‌کارگیری یک آدرس جدید در هر تراکنش، ساز و کارِ بسیار خوبی برای ایجاد حریم خصوصی به وجود آورده است.

بنابراین برای مشاهده موجودیِ حساب[1] یک آدرس موردنظر، درواقع باید موجودی همه UTXO هایی که این آدرس در خروجی آن‌ها قرار دارد را با هم جمع کنیم. وقتی افراد از یک آدرس به چند آدرس مختلف بیت‌کوین ارسال می‌کنند مجموع کل UTXO های موجود در شبکه بیت‌کوین افزایش، و وقتی افراد چند UTXO را با یکدیگر ادغام[2] می‌کنند و خروجی را به یک آدرس ارسال می‌کنند این مقدار کاهش پیدا می‌کند.

مدل UTXO تشخیص دوبار خرج‌کردن[3] را هم بسیار ساده و مؤثر می‌کند چون هر UTXO را فقط یک بار می‌توان خرج کرد. با این روش دیگر نیازی به بایگانی تاریخچه همه پرداخت‌های انجام شده از یک آدرس بیت‌کوین هم نخواهد بود.

1 Balance
2 Consolidate
3 Double spend

همچنین می‌توان با ایجاد تراکنش‌های پیچیده‌ای که ورودی و خروجی‌های مختلف را با هم ترکیب می‌کنند، در آنِ واحد تعداد زیادی UTXO ایجاد کرد و از بین برد. این ویژگی امکان «ترکیب کوین‌ها[1]» را فراهم می‌کند که در آن چندین نفر می‌توانند در یک تراکنش بیت‌کوین، که هرتعدادی از ورودی‌ها را برای تولید هرتعداد خروجی ترکیب می‌کند شرکت، و از این طریق تاریخچه UTXO ها را پنهان کنند. به علاوه این اجازه را به افراد می‌دهد که کوین‌ها را از آدرس‌های مختلف به یک آدرس ادغام کنند یا آن‌ها را بین آدرس‌های مختلف و برای افزایش امنیت و حریم خصوصی پخش کنند.

کیف پول

ایجاد یک حساب، چیزی بیشتر از ساخت یک عدد تصادفی ۲۵۶ بیتی به عنوان کلید خصوصی نیست، و ما می‌توانیم هزاران و یا حتی میلیون‌ها حساب ایجاد کنیم. به همین دلیل نیاز به ساز و کاری برای رصد کردن آن‌ها پیدا می‌کنیم. در بیت‌کوین واژه کیف پول به هرنوع وسیله‌ای اشاره می‌کند که با آن بتوانیم کلیدهای خود را مدیریت کنیم. این وسیله می‌تواند به سادگیِ یک تکه کاغذ باشد و یا به پیچیدگی یک سخت‌افزار.

نرم‌افزار اصلی بیت‌کوین که توسط ساتوشی ارائه شد به همراه خود یک نرم‌افزار کیف پول دارد. این کیف پول قادر است جفت کلیدهای عمومی و خصوصی شما را ایجاد کند. (یادآوری می‌کنم، کلید عمومی برای ساختن آدرس بیت‌کوین 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، بیت‌کوین 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. در آینده کیف پول‌های بیشتری ساخته خواهد شد. هرکسی با دانش

1 Coin mixing

برنامه‌نویسی کامپیوتر می‌تواند کیف پول خود را بسازد یا سورس کُد[1] کیف پول‌ها را بررسی کند تا مطمئن شود هیچ تقلبی در کار نیست. این یکی دیگر از مزیت‌های کیف پول‌های بیت‌کوین بر اپلیکیشن‌های موبایلِ بانکِ شما است که برای نوآوری در این حوزه نیازی به کسب اجازه از یک مرجع مرکزی نیست.

از آنجا که برای خرج کردن کوین‌های‌تان فقط به کلید خصوصی نیاز است، پس باید به خوبی از آن مراقبت کنید. اگر کسی کارت اعتباری شما را سرقت کند، می‌توانید با شرکت صادر کننده آن تماس و با تنظیم شکایت، پول خود را پس بگیرید. در بیت‌کوین، چنین واسطه‌ای وجود ندارد. اگر کسی کلید خصوصی شما را در اختیار داشته باشد می‌تواند کوین‌های 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، به مشکل خواهید خورد. اگر بر اساس روش پیشنهاد شده، برای هر دریافت بیت‌کوین آدرسی جدید می‌سازید و بعد از آن کلیدهای خصوصی را ذخیره و از آن‌ها پشتیبان تهیه می‌کنید، بعد از گذشت مدت کوتاهی این کار برای شما بسیار دشوار خواهد شد.

درطول زمان، راه‌حل‌هایی برای حل این مشکل ارائه شده است. در سال ۲۰۱۲، BIP32 (پیشنهاد بهبود بیت‌کوین[2] سازوکاری است که در آن افراد می‌توانند ایده خود را برای ارتقاء بیت‌کوین منتشر کنند) پیشنهاد ایجاد کیف پول‌های سلسله‌مراتبی-قطعی[3] که به آن HD می‌گویند را مطرح کرد. در این روش تنها با استفاده از یک عدد تصادفی (معروف به seed) می‌توان تمام زنجیره جفت‌کلیدهای عمومی و خصوصی را ایجاد کرد؛ آدرس‌های بیت‌کوین و امضای دیجیتال هرکدام از آنها.

1 Source code
2 Bitcoin Improvement Proposal
3 HD Wallet (Hierarchical Deterministic Wallet)

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 از یک seed نگهداری و پشتیبان‌گیری کنید.

در سال ۲۰۱۳، BIP39 ذخیره و پشتیبان‌گیری از کلیدها را حتی آسان‌تر کرد. به‌جای استفاده از اعدادِ 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، پشتیبان‌گیری از کلیدها بسیار ساده می‌شود. می‌توانید این seed را روی تکه‌ای کاغذ بنویسید و در محل امنی از آن نگهداری کنید. حتی می‌توانید عبارت‌ها را به‌خاطر بسپارید و از کشوری که اقتصاد آن در حال فروپاشی است خارج شوید، و هیچ‌کس متوجه نخواهد شد که همه دارایی شما در ذهن شما ذخیره شده است.

علاوه بر این ممکن است برای دسترسی به بیت‌کوین‌های ذخیره شده در یک آدرس به بیش از یک کلید خصوصی نیاز باشد. آدرس‌های چند امضایی[1] یا multisig می‌توانند انواع مختلفی از طرح‌های امنیتی را به کار گیرند. به عنوان مثال افراد می‌توانند حساب‌های مشترک داشته باشند که ۱-از-۲ باشد، یعنی هریک از آنها می‌تواند تراکنش‌ها را امضا کند یا ممکن است ۲-از-۲ باشد که در این صورت برای جابه‌جا کردن بیت‌کوین‌های ذخیره شده، هر دو طرف باید تراکنش را با کلیدهای خصوصی‌شان امضا کنند.

می‌توان با استفاده از مدل چند امضاییِ ۲-از-۳ یک حساب امانی[2] ایجاد کرد. خریدار و فروشنده هرکدام یک کلید در اختیار دارند و کلید سوم به یک میانجی[3] (حَکَم) اختصاص

1 Multisignature
2 Escrow
3 Arbitrator

پیدا می‌کند. خریدار و فروشنده در صورت توافق بر سر معامله می‌توانند تراکنش را امضا کنند، ولی اگر اختلاف نظری بین آن‌ها پیش آید، نفر سوم می‌تواند با یکی از طرفین توافق و تراکنش را امضا کند.

می‌توانید برای جلوگیری از بروز خطر از دست رفتن کلیدها از مدل ۳-از-۵ استفاده کنید. در این صورت حتی اگر ۲ کلید از ۵ کلید خود را از دست بدهید، همچنان قادر به استفاده از حساب خود خواهید بود. می‌توان ۲ تا از کلیدها را در دو جای مختلف، ۲ تای دیگر را نزد دو دوست قابل اطمینان که یکدیگر را نمی‌شناسند گذاشت، و آخرین کلید را در سرویس‌های خاصی مثل BitGo قرار داد که تراکنش‌های شما را با همکاری شما امضا می‌کنند. با این کار درحالی‌که از خطر از دست رفتن کلیدهای خود جلوگیری می‌کنید، سرقت بیت‌کوین‌های شما نیز بسیار دشوار خواهد بود. (با توجه به شرایط فعلی کشور ما در روابط جهانی، در انتخاب و استفاده از سرویس‌های بین‌المللی نهایت دقت را به‌کار برید. - م)

حتی می‌توان از این هم فراتر رفت و آدرس‌هایی را ساخت که دسترسی به آنها شرایط پیچیده‌تری داشته باشد، مثلاً برای جابه‌جا کردن آن‌ها نیاز به افشای عددی محرمانه باشد، یا اصلاً امکان جابه‌جا کردن آن‌ها برای مدت مشخصی وجود نداشته باشد. مثلا می‌توانید یک آدرس بیت‌کوین بسازید که به مدت ۱۰ سال نتوانید از آن خرج کنید؛ هیچ‌کس نمی‌تواند شما را مجبور به تغییر آن کند.

این گزینه‌ها اثرات عمیقی بر زندگی ما خواهند داشت و می‌توانند دنیا را تغییر دهند. پیش از این هرگز امکان نداشت کسی بتواند دارایی خود را تا این حد مصون از مصادره یا سرقت با خود حمل کند.

فصل ۸

نرم‌افزار بیت‌کوین[1]

تا اینجا یک سیستم توزیع‌شده ساختیم که با آن می‌توان حساب و کتاب پول، و نقل و انتقالات آن را نگه داشت. بیایید آنچه را که ایجاد کرده‌ایم مرور کنیم:

۱. یک دفتر کلِ توزیع‌شده که یک نسخه از آن در اختیار همه اعضا قرار دارد.
۲. یک سیستم قرعه‌کشی براساس اثباتِ کار و ساز و کارِ بازتنظیمِ سختی شبکه برای حفظ ایمنی و ثابت نگه داشتن حجم عرضه بیت‌کوین.
۳. یک سیستم اجماع که این اطمینان را به همه اعضای شبکه می‌دهد که می‌توانند تمام تاریخچه بلاک‌چین را شخصاً و با استفاده از نرم‌افزار متن بازِ بیت‌کوین اعتبارسنجی کنند.
۴. یک سیستم شناسایی بر پایه امضای دیجیتال که اعضا را قادر به ساختن حساب‌های کاربری و دریافت بیت‌کوین بدون نیاز به یک مرجع مرکزی می‌کند.

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

1 Bitcoin client

نرم‌افزار بیت‌کوین

در طول فصل‌های قبل، فرض ما بر این بود که همه اعضا در شبکه از یک قانون پیروی می‌کنند: اجازه دوبار خرج کردن کوین‌ها را نمی‌دهند، اطمینان حاصل می‌کنند که هر بلاک مقدار اثباتِ کار 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 بیت‌کوین یک نرم‌افزار متن باز است. متن باز یعنی هرکسی می‌تواند کُدهای آن را بخواند، و همچنین هرجایی از کُد را که بخواهد برای خود تغییر دهد. اما این تغییرات چگونه به بیت‌کوین راه پیدا می‌کنند؟

بیت‌کوین یک پروتکل[1] است. در نرم‌افزارِ کامپیوتر، این واژه به معنای مجموعه‌ای از قوانین است که نرم‌افزار از آنها پیروی می‌کند. با این حال، شما تا جایی اجازه تغییر دارید که نرم‌افزار شما همچنان مجموعه قوانینی که همه از آن پیروی می‌کنند را رعایت کند. وقتی گفته می‌شود که کسی «یک نود بیت‌کوین اجرا می‌کند»، درواقع به معنای اجرا کردن نرم‌افزاری است که به زبان پروتکل بیت‌کوین حرف می‌زند و قوانین آن را رعایت می‌کند. این نرم‌افزار می‌تواند با سایر نودهای بیت‌کوین ارتباط برقرار کند، تراکنش‌ها و بلاک‌ها را به آنها انتقال دهد، نودهای دیگر را برای وصل شدن به آن‌ها پیدا کند و چیزهایی از این قبیل.

جزئیات نحوه پیاده‌سازی این نرم‌افزار بر عهده کسی است که آن را اجرا می‌کند. درواقع درحال‌حاضر نرم‌افزارهای زیادی پروتکل بیت‌کوین را پیاده‌سازی کرده‌اند. مشهورترینِ آنها `Bitcoin Core` است که نسخه توسعه‌یافته‌ی نرم‌افزاری است که برای اولین بار توسط ساتوشی ناکوموتو منتشر شد.

1 Protocol

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

چه کسی قوانین را تعیین می‌کند؟

قوانینی که بیت‌کوین با آن‌ها تعریف می‌شود در `Bitcoin Core` نوشته شده‌اند، اما چه کسی درمورد قوانین تصمیم می‌گیرد؟ چرا می‌گوییم بیت‌کوین کمیاب است درحالی‌که ممکن است یک نفر تغییری در نرم‌افزار ایجاد کند و تعداد بیت‌کوین را از ۲۱ میلیون به ۴۲ میلیون تغییر دهد؟

چون این سیستم توزیع‌شده است، تمامی نودها در شبکه باید روی این قوانین توافق داشته باشند. اگر یک ماینر نرم‌افزار بیت‌کوین را به‌گونه‌ای تغییر دهد تا دوبرابر آنچه که در قوانین بیت‌کوین آمده جایزه دریافت کند، بقیه نودها بلاک استخراج شده توسط این ماینر را قبول نخواهند کرد. تغییر قوانین بیت‌کوین بسیار سخت است چون هزاران نودِ توزیع‌شده در سراسر جهان هستند که این قوانین را اجرا می‌کنند.

مدل حاکمیت بیت‌کوین به راحتی قابل فهم نیست، به‌خصوص برای کسانی مثل ما که در یک دموکراسی غربی زندگی می‌کنند. ما عادت کرده‌ایم که با رأی دادن حکومت کنیم، رأی 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 بیت‌کوین بیشتر شبیه به آنارشی است تا دموکراسی. بیایید نگاهی به نحوه کنترل این مسئله در سیستم بیندازیم:

نودها: هر عضو در شبکه بیت‌کوین یک نود 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 ساختن بلاک را داشته باشد، طبعا هیچ‌کس آن را اجرا نخواهد کرد. نود، یعنی هرکسی که پذیرنده بیت‌کوین است؛ مانند فروشندگان، صرافی‌ها، ارائه‌دهندگان کیف پول و افرادی که به صورت روزمره از بیت‌کوین استفاده می‌کنند.

ماینرها: بعضی از نودهای شبکه استخراج هم می‌کنند، یعنی برق مصرف می‌کنند تا اجازه نوشتن در دفتر کل بیت‌کوین را داشته باشند. این کار امنیت شبکه بیت‌کوین را تأمین می‌کند؛ چراکه هزینه دستکاری در دفتر کل بسیار زیاد است. چون ماینرها تنها کسانی هستند که در دفتر کل می‌نویسند، ممکن است فکر کنید که آنها هستند که قوانین را تعیین می‌کنند، اما اینطور نیست. آنها فقط قوانین اعمال شده توسط نودهای بیت‌کوین بر شبکه را اجرا می‌کنند. اگر ماینرها شروع به تولید بلاک‌هایی کنند که جایزه اضافی دارند، نودهای دیگر آنها را رد می‌کنند، چون این کار باعث بی‌ارزش شدن ارزش کوین‌ها می‌شود. پس هر کاربری که یک نود 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/سرمایه‌گذاران: کاربران افرادی هستند که مثل نودها (پذیرندگان)، به خرید و فروش بیت‌کوین مشغول هستند. در حال حاضر بسیاری از کاربران نود خودشان را اجرا نمی‌کنند اما به یک نود که توسط ایجادکننده کیف پول‌شان اجرا می‌شود اعتماد می‌کنند، چون ارائه‌دهندگان کیف پول به نیابت از کاربران و طبق خواسته و میل آن‌ها عمل می‌کنند. کاربران هستند که ارزش کوین‌ها را در بازار آزاد تعیین می‌کنند. حتی اگر ماینرها و اغلب پذیرندگانِ سیستم بخواهند با هم تبانی کنند و تغییراتی مثل افزایش نرخ جایزه را در سیستم ایجاد کَنند، کاربران می‌توانند قیمت کوین آن‌ها را پایین بیاورند و شرکت‌های متخلف را از گردونه خارج کنند. اگر روزی بیت‌کوین به چیزی تبدیل شود

که کاربران آن را نمی‌پسندند، یک گروه متعصب از کاربران همیشه می‌توانند نسخه بیت‌کوین خود را فعال نگه دارند.

توسعه‌دهندگان: `Bitcoin Core` مهم‌ترین نرم‌افزار بیت‌کوین است که صدها نفر از بهترین توسعه‌دهندگان و شرکت‌های متخصص در علم رمزنگاری 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، درباره آن اظهار نظر کند و یا پیشنهاد تغییری در کُد 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 نسخه 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 بیت‌کوین درواقع همکاری صدها و هزاران عضو آن است که اگرچه همه آنها خودخواهانه عمل می‌کنند و معمولا در رقابت با یکدیگر هستند، اما در نهایت یک سیستم بسیار مقاوم و به نفع همه ایجاد شده است. بیت‌کوین واقعاً یک بازار آزاد و برپایه آنارشی است که شخص خاصی مسئول آن نیست.

فصل ۹

گذشته، حال و آینده

حالا که شبکه بیت‌کوین را کاملا شناختیم 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 بیت‌کوین‌ها را با استفاده از CPU کامپیوتر خود ماین کرد. چون سختی اولیه سیستم بسیار کم بود، تولید این کوین‌ها با کامپیوتر برای او ارزان درمی‌آمد.

به مرور زمان، با دستکاری نرم‌افزار، عملیات استخراج بهتر و بهتر شد. درنهایت از پردازنده خاصی به نام GPU استفاده شد که روی کارت‌های گرافیکی وجود داشت و برای بازی‌های ویدیویی استفاده می‌شد.

با استفاده از GPU، عملیات استخراج هزاران بار بهتر از CPU انجام می‌شد. در این زمان افرادی که از CPU استفاده می‌کردند کسر کمتری از توان هش شبکه را نسبت به ماینرهای GPU دردست داشتند که با افزایش سختی، ماین کردن برای آن‌ها سودی نداشت.

وقتی GPU بر CPU غالب شدند، مردم شروع به خرید مقدار زیادی از آن‌ها کردند. با تولید ASIC (Application Specific Integrated Circuit) میزان بهره‌وری استخراج بیت‌کوین بهینه‌تر شد. آن‌ها چیپ‌های سخت‌افزاری هستند که تنها یک کار انجام می‌دهند؛ فقط تابع Sha256 بیت‌کوین را اجرا می‌کنند. ASICها فقط این الگوریتم خاص را اجرا می‌کنند و در نتیجه برای عملیات استخراج، هزاران بار به‌صرفه‌تر از GPU هستند و عملاً آنها را غیرقابل استفاده کردند، درست همان کاری که GPU با CPU کرد. هر چندسال یک بار نسل جدیدی از ASIC عرضه می‌شود که با توجه به پیشرفت چشمگیری که در راندمان دارد نسخه‌های قبل از خود را از رده خارج می‌کند.

ماینرهای اولیه در شبکه، برای تولید بیت‌کوین هزینه برق کمی صرف می‌کردند. با افزایش قیمت بیت‌کوین، ماینرهای زیادی به شبکه پیوستند و درنتیجه سختی بالا رفت و تولید بیت‌کوین گران و گران‌تر شد.

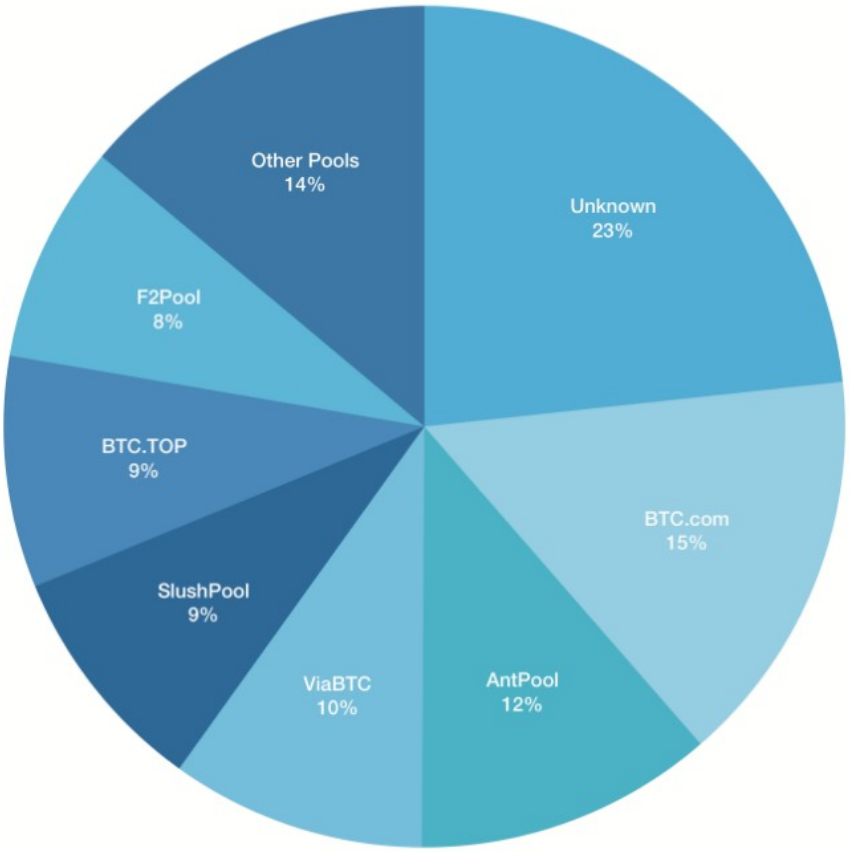
یک مسئله در استخراج بیت‌کوین این است که قطعیت ندارد. مثل پرتاب تاس است. یعنی شما ممکن است صدها دلار برای مصرف برق هزینه کنید و هیچ بلاک معتبری هم پیدا نکنید.

در سال ۲۰۱۰ ابتکار تازه‌ای به نام استخر استخراج[1] ایجاد شد تا مشکل ماینرهایی را که انرژی مصرف می‌کنند اما جایزه‌ای دریافت نمی‌کنند حل کند. استخر استخراج چیزی شبیه به بیمه‌های درمانی است و ریسک کار را به اشتراک می‌گذارد.

همه ماینرهای استخر در کار استخراج با یکدیگر مشارکت می‌کنند و 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 توان هش‌ای که در اختیار استخر گذاشته‌اند، تقسیم می‌شود. این باعث می‌شود که حتی ماینرهای کوچک مثل ماینرهای شخصی هم با

1 Mining Pool

توجه به میزان مشارکت‌شان در توان هش، مقدار کمی جایزه دریافت کنند. برای ایجاد این سرویس، استخر بخشی از جایزه ایجاد بلاک را به‌عنوان کارمزد دریافت می‌کند.
ظهور استخرهای استخراج باعث ایجاد تمرکز در شبکه شده است، چون کاربران به سمت استخرهای بزرگتر می‌روند. نمودار زیر توزیع تقریبی استخرها را در ژانویه ۲۰۱۹ نشان می‌دهد.



حمله‌های ۵۱٪

تمرکز در استخرهای استخراج باعث نگرانی درمورد حمله ۵۱٪ در شبکه می‌شود. اگر به نمودار بالا نگاه کنید، متوجه خواهید شد که مجموع توان هشِ ۵ استخر برتر آن، بیش از ۵۰٪ کل شبکه است.

بیایید بررسی کنیم که چنین حمله‌ای چگونه اتفاق می‌افتد و چه خطراتی به همراه دارد.

وقتی بیش از ۵۰٪ از توان هشِ شبکه دراختیار شما باشد، شما بر ثبت بلوک‌ها در دفتر کل تسلط کامل خواهید داشت، چون توانایی شما در تولید زنجیره‌ی طولانی‌تر بیشتر از ۵۰٪ از سایر اعضای شبکه است. توجه داشته باشید که اجماع ناکاموتو می‌گوید که باید زنجیره‌ای را بپذیریم که شامل طولانی‌ترین زنجیره اثباتِ کار باشد.

در اینجا مثالی ساده از نحوه رخ دادن حمله ۵۱٪ ارائه می‌کنیم:

۱. فرض می‌کنیم شبکه در کل ۱,۰۰۰ هش در هرثانیه تولید می‌کند و بلوک‌ها را در دفتر کل می‌نویسد.
۲. شما مقداری سخت‌افزار استخراج و برق خریداری می‌کنید که بتوانید ۲,۰۰۰ هش برثانیه تولید کنید. حالا شما ۶۶٪ از کل توان هش را دراختیار دارید(۲۰۰۰/۳۰۰۰).
۳. شما شروع به استخراج زنجیره‌ای می‌کنید که فقط شامل بلاک‌های خالی است.
۴. دوهفته بعد زنجیره بلوک‌های خالیِ خود را در شبکه منتشر می‌کنید. چون توان استخراج شما دوبرابر سریع‌تر از ماینرهای صادق شبکه است پس زنجیره شما دو برابر طولانی‌تر از بقیه شبکه خواهد بود و در تمام شبکه پذیرفته خواهد شد و تاریخچه ۲ هفته گذشته از بین خواهد رفت.

علاوه بر استخراج بلاک‌های خالی که زنجیره را بلااستفاده می‌کنند، می‌توانید حمله دوبار خرج کردن را هم ترتیب دهید:

۱. تعدادی بیت‌کوین به یک صرافی ارسال کنید.
۲. آن را با بفروشید و پول را از صرافی برداشت کنید.
۳. بعد از مدتی، زنجیره‌ای را که مخفیانه ساخته‌اید و تراکنش ارسال بیت‌کوین به صرافی در آن نوشته نشده است را در شبکه منتشر کنید.
۴. شما حالا زنجیره را بازنویسی کرده‌اید و هم بیت‌کوین‌ها و هم پول‌ها برای شما است.

در عمل، با توان هش‌ای که امروزه در شبکه وجود دارد، فراهم آوردن برق و سخت‌افزار لازم برای ترتیب دادن چنین حمله‌ای بسیار گران است (یادآوری می‌کنم که مصرف برق شبکه بیت‌کوین در حال حاضر به اندازه یک کشور متوسط است). همچنین، از بین بردن شواهد در حمله دوبار خرج کردن با این روش بسیار سخت است و ترتیب‌دهندگان آن در نهایت شناسایی خواهند شد (معمولاً خرید و فروش بیت‌کوین در ارقام بالا نیاز به احراز هویت دارد. – م). از این‌ها گذشته، شما باید به اندازه یک کشور متوسط انرژی مصرف کنید و میلیون‌ها دلار بابت خرید سخت‌افزار بپردازید، سپس میلیون‌ها دلار را برای فروش به صرافی ارسال کنید.

انجام چنین حمله‌ای در بازه زمانی طولانی که باعث بروز مشکل در شبکه بیت‌کوین شود تقریباً غیرممکن است ولی حتی اگر فرض کنیم گروهی یا افرادی به یک بودجه نامحدود دسترسی داشته باشند و بخواهند برای آسیب رساندن به شبکه بیت‌کوین به این حمله ادامه دهند، شبکه می‌تواند یک روش جدید اثباتِ کار را به خدمت بگیرد (چیزی متفاوت از sha256). در این صورت همه سخت‌افزارهای ASIC که توسط مهاجم استفاده شده‌اند

بلااستفاده خواهند شد. اگرچه این گزینه باعث ناکارآمد شدن تمام ماینرهای صادق نیز می‌شود اما شبکه زنده می‌ماند و دوباره روی پای خود خواهد ایستاد.

علاوه بر غیرممکن بودن حمله ۵۱ درصد، حتی با فرض دردست داشتن اکثریت توان هشِ شبکه، هیچ‌یک از موارد زیر در شبکه عملی نخواهد بود:

۱. نمی‌توان سرخود و به‌عنوان پاداشِ ایجادِ بلاک، خارج از برنامه زمان‌بندی شده از هیچ، بیت‌کوین اضافی تولید کرد. چون برنامه زمان‌بندی ایجاد بلاک‌ها را نقض خواهد کرد و حتی اگر بلاک دارای اثباتِ کار کافی باشد، نودهای شبکه آن را رد می‌کنند.
۲. امکان خرج کردن کوین‌هایی که مالک آن‌ها نیستید همچنان وجود ندارد، چون باید یک امضای دیجیتال معتبر ارائه دهید.
۳. نمی‌توان سرعت عرضه بیت‌کوین را بالا برد، چون سختی مثل قبل، هر ۲۰۱۶ بلاک تنظیم می‌شود.

درنتیجه حتی اگر اکثریت ماینرها متقلب باشند، نودهای پذیرنده بیت‌کوین می‌توانند از درستیِ شبکه محافظت کنند. علاوه بر این اگر یک استخر استخراج درصد خاصی از توان هش شبکه را دراختیار دارد به این معنی نیست که همه سخت‌افزار موجود در آن، در اختیار این استخر است. 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 بیت‌کوین هستند. ماینرها برای کسب درآمد تلاش می‌کنند نه برای ازدست دادن آن.

در گذشته اتفاق افتاده است که ماینرها استخر استخراجی که توان هش آن زیاد شده بود را ترک کردند. در سال ۲۰۱۴، Ghash.io نزدیک به نیمی از قدرت شبکه را دردست

داشت. ماینرها متوجه شدند که شبکه به سمت متمرکز شدن پیش می‌رود، پس داوطلبانه استخر را ترک کردند.

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

هارد فورک‌ها[1] و سافت فورک‌ها[2]

پیچیده‌ترین موضوع در بیت‌کوین را در مرحله آخر توضیح می‌دهیم.

تا اینجا متوجه شدیم که نرم‌افزار بیت‌کوین چگونه قوانینی را که افراد روی آن‌ها توافق دارند در شبکه اعمال می‌کند و فهمیدیم که افراد چگونه قوانینی را که موافق آن هستند با استفاده از انتخاب نسخه نرم‌افزار اجرا می‌کنند.

همچنین توضیح دادیم که چطور ماینرها درهنگام تولید بلاک قوانین شبکه را رعایت می‌کنند و باید بلاک‌ها را به گونه‌ای تولید کنند که مورد قبول کاربران باشد، در غیر این صورت باید ریسک رد شدن بلاک و از دست رفتن پاداش بلاک را بپذیرند.

درنهایت، می‌دانیم که نرم‌افزار بیت‌کوین طولانی‌ترین زنجیره‌ای که بیشترین حجم انباشته اثباتِ کار را در خود جای داده باشد به عنوان زنجیره معتبر می‌پذیرد، و می‌دانیم که چند شاخه شدن زنجیره‌ها (یا به‌اصطلاح فورک‌ها) به دلایلی که در فصل ۶ به تفصیل توضیح داده شد اتفاق می‌افتند.

1 Hard Fork
2 Soft Fork

حالا بیایید به فورک‌هایی که به عمد ایجاد می‌شوند بپردازیم. فورکِ عمدی زمانی‌ست که تعدادی از ماینرها و/یا کاربران با قوانین جاری بیت‌کوین موافق نباشند و تصمیم بگیرند آن را تغییر دهند. به‌طور کلی دو نوع فورک برای تغییر قوانین وجود دارد: سافت فورک، که با قوانین قبل سازگاری دارد[1] و هارد فورک که با قوانین قبل سازگار نیست[2]. ببینیم این فورک‌ها چطور اتفاق می‌افتند و مثال‌هایی از آنها را مطرح کنیم.

سافت فورک‌ها

یک سافت فورک ایجاد تغییر در قوانین اجماع بیت‌کوین است، به صورتی که تغییرات با قوانین قبلی شبکه سازگاری داشته باشد. یعنی چه؟ این یعنی اگر شما یک نود قدیمی را اجرا کنید که به‌روزرسانی نشده باشد، بلاک‌هایی که با قوانین جدید ساخته شده‌اند همچنان برای نود شما معتبر هستند. برای یک نود که با فورک جدید به‌روزرسانی شده است تمام بلاک‌هایی که قبلا نامعتبر بوده‌اند هنوز هم نامعتبر هستند اما حالا بعضی از بلاک‌های معتبر ممکن است برای این نود نامعتبر باشند. اجازه دهید با یک مثال این موضوع را روشن‌تر کنیم:

۱۲ سپتامبر ۲۰۱۰ قانون جدیدی به نرم‌افزار بیت‌کوین معرفی شد: سایز بلاک‌ها حداکثر می‌تواند ۱ مگابایت باشد. این قانون برای مقابله با اسپم‌ها در بلاک‌چین اعمال شد. قبل از این قانون، بلاک‌ها با هر سایزی قابل قبول (معتبر) بودند. با قانون جدید تنها بلاک‌های با اندازه کوچکتر از ۱ مگابایت پذیرفته می‌شدند. اگر شما یک نود قدیمی را اجرا می‌کردید که به‌روزرسانی نشده بود بلاک‌های کوچکتر همچنان برای آن معتبر بودند، پس شما تحت تاثیر قرار نمی‌گرفتید.

استفاده از سافت فورک‌ها برای به‌روزرسانی قوانین شبکه باعث بروز اختلال در شبکه نمی‌شود. چون به صاحبان نودها این امکان را می‌دهد که داوطلبانه و به مرور زمان نرم‌افزار

1 Backwards compatible
2 Backwards incompatible

نود خود را به‌روزرسانی کنند. اگر این کار را هم انجام ندهند، می‌توانند همچنان مثل گذشته به فعالیت خود ادامه دهند. فقط ماینرها که بلاک‌ها را تولید می‌کنند باید نرم‌افزار نود خود را به‌روز کنند تا بلاک‌های تولیدشده از قوانین جدید پیروی کنند. وقتی یک ماینر قانونِ محدودیت ۱ مگابایت را در فورک جدید به‌روزرسانی می‌کرد، سایز تمام بلاک‌های بعدی او حداکثر ۱ مگابایت بود و ممکن بود کاربرانی که نسخه‌های قدیمی نرم‌افزار را اجرا می‌کردند اصلاً از قضیه خبردار نمی‌شدند.

هارد فورک‌ها

هارد فورک نقطه مقابل سافت فورک است. در یک هارد فورک تغییری که با قوانین گذشته سازگار نیست در شبکه اعمال می‌شود و بلاک‌هایی که قبلاً نامعتبر بودند حالا در شبکه معتبر خواهند بود. در یک هارد فورک نودهای قدیمی که به‌روزرسانی نشده‌اند دیگر نمی‌توانند بلاک‌هایی را که تحت قوانین جدید ایجاد شده‌اند بررسی کنند. به همین دلیل تا نرم‌افزار خود را به‌روزرسانی نکنند در زنجیره قبلی باقی خواهند ماند. یکی از نمونه‌های هارد فورک افزایش سایز بلاک‌ها از ۱ مگابایت به سایز بیشتری بود. چون بلاک بزرگ‌تر از ۱ مگابایتی که بر اساس قانون قبلی نامعتبر بود، بعد از اعمال هارد فورک و بر اساس قوانین جدید معتبر است.

هارد فورک‌هایی که در آن‌ها همه نودهای شبکه روی تغییرات جدید با یکدیگر هم رأی هستند، در شبکه مشکلی ایجاد نمی‌کنند. همه نودها باید سریعاً نرم‌افزار خود را به‌روزرسانی کنند. اگر کسی در جریان نباشد و از ایجاد تغییرات در قوانین اطلاع نداشته باشد، دیگر بلاک‌های جدید را دریافت نخواهد کرد و اگر خوش‌شانس باشد متوجه می‌شود که نرم‌افزار ازکار افتاده است و وادار به ارتقاء نرم‌افزار خود خواهد شد.

هارد فورک‌ها درعمل به این سادگی پیش نمی‌روند. در یک سیستم آنارشیستی و غیرمتمرکز، نمی‌توان همه را وادار به قبول قوانین جدید کرد. در اگوست ۲۰۱۷، افرادی که از شرایط بیت‌کوین در زمینه پرداخت‌های ارزان (با کارمزد کم) ناراضی بودند،

تصمیم گرفتند برای ایجاد زنجیره‌ای با بلاک‌های بزرگ‌تر یک فورک ایجاد کنند. چون قانون بیت‌کوین تولید بلاک‌هایی کمتر از ۱ مگابایت بود (با توجه به سافت فورک سال ۲۰۱۰)، این افراد تصمیم گرفتند زنجیره جدیدی ایجاد کنند که در آن اندازه بلاک‌ها بزرگتر باشد. این فورک با نام Bitcoin Cash شناخته می‌شود.

هارد فورکی مثل Bitcoin Cash که از چهارچوب قوانین بیت‌کوین خارج شده است و از جانب همه نودها و ماینرها پذیرفته نمی‌شود، یک بلاک‌چین جدید ایجاد می‌کند که قسمتی از تاریخچه آن با زنجیره اولیه مشترک است، اما از نقطه‌ای که زنجیره آن از زنجیره بیت‌کوین جدا شده است، کوین‌هایی که در آن تولید می‌شوند دیگر بیت‌کوین نیستند و بنابراین توسط هیچ نودی در شبکه بیت‌کوین پذیرفته نخواهند شد.

اینکه چه چیزی بیت‌کوین «است» و چه چیزی بیت‌کوین «نیست» در طی یک سال بعد از فورک Bitcoin Cash بحث داغی بود. بعضی از افرادی که طرفدار Bitcoin Cash بودند، اعتقاد داشتند که بیت‌کوین باید براساس آنچه که ساتوشی ۱۰ 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 مشخصی عمل می‌کند.

درمورد این فورک، اکثریت افرادی که نودهای مهمی از نظر اقتصادی اجرا می‌کردند (مثل کیف پول‌ها، صرافی‌ها و پذیرندگان بیت‌کوین) نمی‌خواستند نرم‌افزار خود را با چیزی که گروه کمتری از آن حمایت می‌کنند و تیم کم‌تجربه‌تری آن را توسعه داده است عوض کنند. همین‌طور میزان توان هشِ شبکه ناچیز آن نشان می‌داد افراد کمتری خواهان تغییر این قوانین هستند. همچنین افراد فکر می‌کردند که چنین «ارتقاءای» ارزش برهم زدن اکوسیستم را ندارد. مشکل هارد فورک‌ها این است که آنها زمانی موفقیت‌آمیز هستند که همه آن را بپذیرند، ولی اگر اختلاف نظر به‌وجود بیاید، دو کوین متفاوت ایجاد

می‌شود. پس بیت‌کوین همان بیت‌کوین باقی ماند و Bitcoin Cash، کوین جداگانه‌ای شد.

امروزه تعداد زیادی فورک بیت‌کوین ایجاد شده است، مثلBitcoin Gold و Bitcoin Diamond وBitcoin Private، که توان هشِ شبکه ناچیزی امنیت آنها را تامین می‌کند و توسعه‌دهندگان کمتری مشغول توسعه آن‌ها هستند و تقریبا فعالیت اقتصادی ندارند. بسیاری از آنها به طور واضحی مصداق کلاه‌برداری، یا پروژه‌های تحقیقاتی سطح پایینی هستند. صدها کوین شبیه به بیت‌کوین وجود دارند که کدهای مشابهی دارند اما تاریخچه حساب (مجموعه UTXO) آن‌ها از بیت‌کوین جدا است، مثل Litecoin و Dogecoin.

بازار کارمزد تراکنش

درباره کارمزد در فصل ۵ وقتی درباره استخراج بیت‌کوین صحبت می‌کردیم بحث کوتاهی شد ولی این مسأله می‌بایست در یک بخش جداگانه توضیح داده شود. در برنامه عرضه بیت‌کوین، هر ۴ سال یک‌بار مقدار پاداش تولید بلاک‌ها نصف می‌شود تا زمانی‌که کاملا حذف شود و از آن به بعد هیچ‌گونه عرضه جدیدی در بیت‌کوین نخواهد بود. اما ما همچنان باید راهی پیدا کنیم تا برای حفظ امنیت شبکه به ماینرها انگیزه کافی بدهد.
کارمزد تراکنش توسط بازار آزاد تعیین می‌شود، که در آن کاربران برای خرید فضای محدودِ بلاک به ماینرها 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 دهند یا نه. زمانی که تعداد تراکنش‌های در صف انتظار کم باشد، مقدار کارمزد می‌تواند به مقدار کم تعیین شود چون رقابتی وجود ندارد. اما با پر شدن فضای بلاک، کاربرانی که می‌خواهند تراکنش‌شان سریع‌تر تایید شود (در بلاک بعدی قرار بگیرد) 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 انتقال یافته است، در بیت‌کوین مبلغ منتقل‌شده بر کارمزد هیچ تاثیری ندارد. درعوض، کارمزد متناسب با منابع محدودی که مصرف می‌شوند (یعنی فضای بلاک) تعیین می‌شود. بنابراین کارمزد با واحد «ساتوشی بر بایت[1]» اندازه‌گیری می‌شود (هر بایت برابر با ۸ بیت است. درواقع فقط مقدار فضایی که تراکنش شما اشغال می‌کند را اندازه‌گیری می‌کند). درنتیجه کارمزد تراکنشی که یک میلیون بیت‌کوین را به یک آدرس ارسال می‌کند ارزان‌تر از تراکنشی است که یک بیت‌کوین را به ۱۰ قسمت تقسیم می‌کند و آن‌ها را به ۱۰ حساب جداگانه ارسال می‌کند، چون دومی فضای بیشتری در بلاک اشغال می‌کند.

در گذشته، در برهه‌ای از زمان که بیت‌کوین خریداران زیادی داشت، مثل زمان افزایش قیمت اواخر سال ۲۰۱۷، کارمزدها بسیار بالا رفت. بعد از آن امکانات جدیدی برای کاهش فشار کارمزد در شبکه پیاده شد.

یکی از این امکانات Segregated Witness یا Segwit است که ساختار بلاک را تغییر می‌دهد و با جدا کردن امضای دیجیتال از تراکنش‌ها فضای بیشتری برای داده‌ها بوجود می‌آورد. تراکنش‌هایی که از این قابلیت استفاده می‌کنند، می‌توانند بیشتر از ۱ مگابایت فضای بلاک را اشغال کنند و توضیح این ترفند هوشمندانه از حوصله این کتاب خارج است.

عامل دیگر کاهش کارمزدها به‌دلیل ارسال گروهی تراکنش‌ها است. صرافی‌ها و دیگر عوامل تاثیرگذار در اکوسیستم بیت‌کوین که حجم تراکنش‌های بالایی دارند، اقدام به ترکیب تراکنش‌های چندین کاربر بیت‌کوین در یک تراکنش کردند. برخلاف سیستم

1 Satoshis per byte

پرداخت سنتی در بانک یا پِی‌پال که تراکنش‌ها از یک فرد به فرد دیگر است، یک تراکنش بیت‌کوین می‌تواند تعداد زیادی ورودی را با هم ترکیب کند و تعداد زیادی خروجی تولید کند. بنابراین یک صرافی که باید برای ۱۰۰ نفر بیت‌کوین 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 تراکنش‌ها هم‌اکنون به‌خوبی تقاضا برای فضای بلاک را کاهش داده‌اند و اصلاحات بیشتری هم برای استفاده بهینه از فضای بلاک درحال توسعه است. با این‌حال زمانی فرا خواهد رسید که کارمزد بیت‌کوین به دلیل پر شدن بلاک‌ها در اثر تقاضای زیاد کاربران، دوباره بالا خواهد رفت.

تحولات آینده بیت‌کوین

تا اینجا پروتکل بیت‌کوین را اختراع کردیم و به چگونگی تکامل شبکه درطول زمان پرداختیم. حالا می‌خواهیم به آینده نگاه کنیم و برخی از پیشرفت‌هایی که به‌زودی در بیت‌کوین رخ می‌دهند را بررسی کنیم.
برخلاف ارز سنتی، که چاپ و استفاده می‌شود، بیت‌کوین یک پول قابل برنامه‌نویسی است که می‌توان روی آن لایه‌های خدماتی بی‌شماری ایجاد کرد. این یک مفهوم کاملاً جدید است و ما تازه اول راه هستیم.

شبکه لایتنینگ[1]

همان‌طور که گفته شد، مشکل بیت‌کوین این است که با افزایش تقاضا برای فضای خالی بلاک، کارمزد تراکنش‌ها هم افزایش می‌یابد. امروزه بیت‌کوین بر اساس تعداد تراکنش‌هایی که در یک بلاک جا می‌شوند می‌تواند بین ۳ تا ۷ تراکنش درثانیه انجام دهد. به این نکته توجه کنید که اگرچه هر تراکنش ممکن است از طریق دسته‌بندی،

1 Lightning Network

درواقع پرداخت به صدها نفر باشد اما همچنان ظرفیت کافی برای تبدیل شدن به یک شبکه پرداخت جهانی را ندارد.

یک راه حل ساده لوحانه می‌تواند افزایش سایز بلاک باشد و در واقع چندین رقیبِ بیت‌کوین مثل Bitcoin Cash این روش را امتحان کرده‌اند. اما بیت‌کوین این راه را در پیش نخواهد گرفت چون افزایش سایز بلاک می‌تواند بر خصوصیات غیرمتمرکزِ شبکه مثل تعداد نودها و پراکندگی جغرافیایی آنها تاثیر منفی بگذارد. حتی اگر افزایش سایز بلاک با پیشرفت‌هایی که در سخت‌افزار رخ می‌دهد ممکن باشد، همچنان ذات غیرمتمرکز بیت‌کوین ممکن است در مقابل هارد فورکی که قصد افزایش سایز بلاک را داشته باشد طوری برخورد کند که باعث ایجاد اخلال و بی‌نظمی در اکوسیستم شود و دوباره موجب پدید آمد یک زنجیره و کوین جدید شود.

همچنین افزایش سایز بلاک‌ها مشکل مناسب نبودن بیت‌کوین به عنوان یک سیستم پرداخت جهانی را نیز حل نمی‌کند چون افزایش ظرفیت تراکنش‌های شبکه بیت‌کوین به این سادگی‌ها نیست. شبکه لایتنینگ برای حل این مشکل معرفی شده است؛ یک پروتکل جدید و مجموعه‌ای از نرم‌افزارهای پیاده‌سازی شده‌ای که تراکنش‌های بیت‌کوینی را به صورتoff-chain (خارج از زنجیره بیت‌کوین) ایجاد می‌کند. شبکه لایتنینگ به تنهایی می‌تواند موضوع یک کتاب باشد، اما اینجا توضیح مختصری درباره آن می‌دهیم.

ایده لایتنینگ این است که نیازی به ثبت همه تراکنش‌ها در بلاک‌چین نیست. برای مثال اگر من و شما به یک کافه برویم و نوشیدنی سفارش بدهیم، فروشنده حساب سفارش‌های ما را تا آخر پیش خود نگه می‌دارد و ما آخر شب و هنگام ترک آنجا حساب‌مان را تسویه می‌کنیم. معنی ندارد حین هربار سفارش دادن حساب‌مان را تسویه کنیم و کارت بکشیم چون این روش فقط وقت ما را تلف می‌کند. شبکه بیت‌کوین ظرفیت ثبت تراکنش‌های خرید قهوه یا نوشابه افراد را روی بلاک‌چینی که به اندازه یک کشور انرژی

مصرف می‌کند و دفتر کل را روی هزاران کامپیوتر در سراسر دنیا ذخیره می‌کند ندارد. علاوه بر این، این روش به حریم خصوصی خریداران هم آسیب می‌رساند.

اگر شبکه لایتنینگ موفق شود، نقاط ضعف زیادی در بیت‌کوین بهبود پیدا خواهند کرد:

- توان عملیاتی تقریبا نامحدود: صدها و هزاران تراکنش کوچک بیت‌کوین می‌توانند انجام و سپس فقط یکبار به عنوان پرداخت نهایی در بلاک‌چین بیت‌کوین ثبت شوند.
- تاییدهای سریع: نیاز نیست صبر کنیم تا بلاک‌ها ساخته شوند.
- کارمزدهای بسیار پایینی که برای پرداخت‌های خُرد مناسب هستند، مثل پرداخت مبلغ کمی برای خواندن مطلب یک وبلاگ.
- افزایش حریم خصوصی: فقط افرادی که در تراکنش شرکت دارند از آن اطلاع پیدا می‌کنند، درست برعکس تراکنش‌های on-chain (که روی بلاک‌چین بیت‌کوین ثبت می‌شوند) و درسراسر شبکه منتشر می‌شوند.

لایتنینگ از مفهوم کانال پرداخت استفاده می‌کند، که درواقع همان تراکنش‌های on-chain هستند که مبلغی بیت‌کوین در آن قرار می‌گیرد و سپس توسط شبکه لایتنینگ سریع و تقریبا رایگان منتقل می‌شود. شبکه لایتنینگ در مراحل اولیه است اما با این وجود آینده روشنی دارد. می‌توانید سایت https://yalls.org که از پرداخت‌های خُرد لایتنینگ برای مطالعه مقالات استفاده می‌کند را ببینید.

بیت‌کوین در فضا

بیت‌کوین مقاومت خوبی در مقابل سانسور دارد. همچنین مصادره آن هم کار آسانی نیست (می‌توانید آن را در ذهن خود نگه‌داری کنید). انتقال آن هم فقط به یک ماینر

صادق در شبکه نیاز دارد تا تراکنش ارسالی شما را تأیید کند (هرکس خودش می‌تواند به استخراج بیت‌کوین بپردازد).

با این حال چون بیت‌کوین از طریق اینترنت جابه‌جا می‌شود، در سطح شبکه درمعرض سانسور قرار دارد. دولت‌ها اگر بخواهند فعالیت بیت‌کوین را کاهش دهند می‌توانند از ورود ترافیک بیت‌کوین به کشورشان جلوگیری کنند.

ماهواره‌ی شرکت «بلاک‌استریم[1]» اولین تلاش برای حذف سانسور در سطح شبکه و ایجاد دسترسی برای مناطق دورافتاده‌ای که به اینترنت دسترسی ندارند است. این ماهواره به همه این امکان را می‌دهد که با یک دیش و مجموعه‌ای از تجهیزات ارزان به شبکه بیت‌کوین متصل شوند و بلاک‌چین آن را دانلود کنند. ارتباط دوطرفه هم به‌زودی امکان‌پذیر خواهد شد. تلاش‌های دیگری هم مثل TxTenna برای ساخت شبکه مش[2] مستقل از اینترنت وجود دارند که وقتی در کنار این سیستم ماهواره‌ای به‌کار گرفته شوند متوقف کردن آن‌ها تقریباً غیرممکن خواهد بود.

1 Blockstream
2 Mesh Networking

فصل ۱۰

قدم بعدی چیست؟

تمام ماجرا همین بود، مراحل اختراع بیت‌کوین 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 بیت‌کوین:

- 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 :

- The Bitcoin whitepaper by Satoshi 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 بیت‌کوین:

- 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 بیت‌کوین در توئیتر است، در اینجا تعدادی از افرادی که دنبال کردن آنها مفید است ذکر شده‌اند. این افراد در آدرس زیر لیست شده‌اند و توسط نویسنده این کتاب به‌روزرسانی می‌شوند:

http://bitcoinerlist.com

درباره نویسنده

Yan Pritzker در ۲۰ سال گذشته یک توسعه‌دهنده نرم‌افزار و کارآفرین بوده است. از سال ۲۰۱۲ تا ۲۰۱۸ او CTO سایت Reverb.com بوده و تکنولوژی و زیرساخت‌های این مجموعه را مدیریت کرده است. امروزه او تمرکز خود را بر آموزش بیت‌کوین و مشاوره برای استارتاپ‌های نوپا گذاشته است.
مطالب نویسنده درباره بیت‌کوین و موضوعات مرتبط در سایت yanpritzker.com قرار می‌گیرد.

همچنین می‌توانید او را در توییتر دنبال کنید: @skwp

ترجمه این کتاب توسط مترجم ناشناس با شناسه توئیتر nodrunner و بازبینی و صفحه‌بندی ویراست اول آن توسط «سایت خبری-آموزشی کوین‌ایران»، و بازبینی و صفحه‌بندی ویراست دوم توسط «سایت منابع فارسی بیت‌کوین» انجام شده است.

منابع فارسی بیت‌کوین
ویراست سوم
بهار ۱۴۰۰