دانشگاه صنعتی شریف
دانشکدهٔ مهندسی کامپیوتر

یادداشت درس مبانی و کاربردهای زنجیرهٔ بلوکی

اثبات کار

نگارش

فاطمه حمدی و فاطمه علیمرادی

استاد درس

دکتر امیرمهدی صادق‌زاده

تابستان ۱۴۰۵

فهرست مطالب

۷ **اثبات کار** ۱

۱.۷ تکثیر لیسا ۳

۱.۱.۷ برخورد بلوک‌ها ۴

۲.۱.۷ انتخاب اعداد خوش‌شانس ۵

۳.۱.۷ احتمال انشعاب‌ها ۱۱

۲.۷ واداشتن ماینرها به انتخاب صادقانهٔ اعداد خوش‌شانس ۱۴

۱.۲.۷ تولید اثبات کار معتبر ۱۶

۲.۲.۷ چرا این روش مفید است؟ ۲۱

۳.۲.۷ مقایسه با اعداد خوش‌شانس ۲۲

۴.۲.۷ اگر نانس‌ها تمام شوند چه؟ ۲۴

۳.۷ ماینرها باید نقل مکان کنند ۲۵

۱.۳.۷ افزودن نرخ هش بیشتر ۲۶

۲.۳.۷ مشکلات نرخ بالای تولید بلوک ۲۷

۳.۳.۷ چه چیزی برطرف شده است؟ ۲۸

۴.۷ تنظیم سختی ۲۹

۱.۴.۷ قواعد مهر زمانی ۳۱

۲.۴.۷ قدرت زنجیره در برابر طول زنجیره ۳۳

۵.۷ ماینرها چه آسیب‌هایی می‌توانند وارد کنند؟ ۳۴

۱.۵.۷ خرج مضاعف ۳۴
۲.۵.۷ محافظت در برابر حملات خرج مضاعف ۳۷
۶.۷ کارمزد تراکنش ۴۵
۱.۶.۷ بلوک‌های بزرگ‌تر کندترند ۴۷
۲.۶.۷ اما موضوع، کارمزد تراکنش نبود؟ ۴۸
۳.۶.۷ اندازهٔ بلوک محدود است ۵۱
۴.۶.۷ وقتی یارانهٔ بلوک صفر می‌شود ۵۳
۷.۷ مرور فصل ۵۴
۱.۷.۷ تغییرات سامانه ۵۶
۸.۷ تمرین‌ها ۵۷
۱.۸.۷ گرم‌کردن ۵۷
۲.۸.۷ مطالعهٔ عمیق‌تر ۵۹
۹.۷ خلاصه ۶۰

مراجع ۶۱

فصل ۷

اثبات کار

این فصل شامل موارد زیر است:

- مقاوم‌سازی تراکنش‌ها[۱] در برابر سانسور، از طریق امکان‌پذیر کردن حضور چندین «لیسا»
- رقابت برای تولید بلوک[۲] بعدی، یا استخراج‌کردن[۳]
- درک انگیزه‌های استخراجگرها[۴]

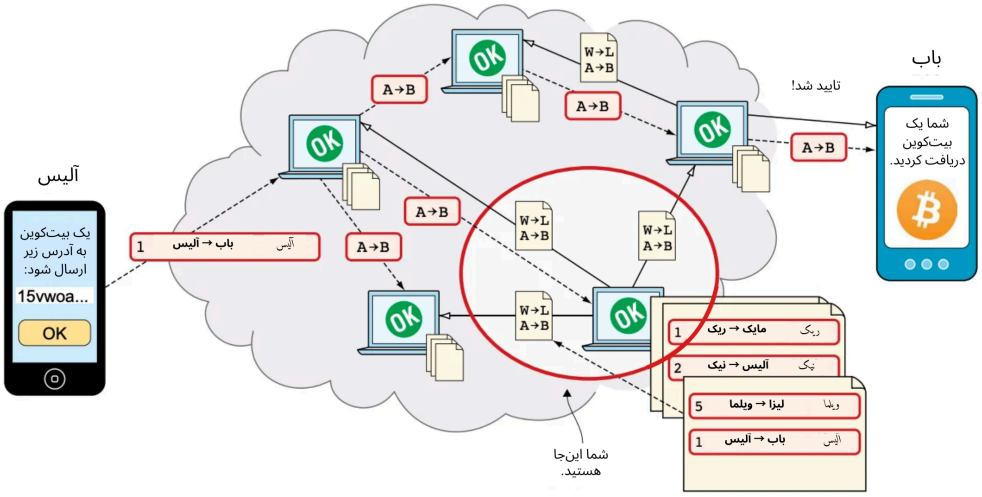
در فصل قبل، با معرفی بلاک‌چینی[۵] که لیسا همهٔ بلوک‌های آن را امضا می‌کرد، حذف تراکنش‌ها را برای او دشوار کردیم. در این فصل، یک گام جلوتر می‌رویم و سامانه را در برابر سانسور مقاوم می‌کنیم تا لیسا نتواند تراکنش‌ها را سانسور کند.

برای مقاوم‌سازی سامانه در برابر سانسور، امضاهای دیجیتال[۶] موجود در سرآیند[۷] بلوک‌ها را با اثبات کار[۸] جایگزین می‌کنیم (شکل ۱.۷). این کار امکان حضور هر تعداد لیسا، یا استخراجگر، را فراهم می‌کند. این استخراجگرها برای ایجاد بلوک بعدی با یکدیگر رقابت می‌کنند و می‌کوشند یک اثبات کار معتبر تولید کنند. استخراجگرها

[۱] Transaction – معادل فارسی: تراکنش
[۲] Block – معادل فارسی: بلوک
[۳] Mining – معادل فارسی: ماین‌کردن/استخراج‌کردن
[۴] Miner – معادل فارسی: استخراجگر/ماین کننده
[۵] Blockchain – معادل فارسی: زنجیرهٔ بلوکی
[۶] Digital signatures – معادل فارسی: امضاهای دیجیتال
[۷] Header – معادل فارسی: سرآیند
[۸] Proof of Work (PoW) – معادل فارسی: اثبات کار

می‌توانند با محاسبهٔ حجم بسیار زیادی ازچکیده‌های[۹] رمزنگاری، این اثبات را تولید کنند. اکنون کیف پول‌ها[۱۰] می‌توانند تراکنش‌های خود را برای هر یک یا همهٔ استخراجگرها ارسال کنند تا از پردازش شدن تراکنش‌هایشان مطمئن شوند.

با استقرار سامانهٔ جدید اثبات کار، استخراجگرها تمایل دارند بلوک‌ها را تا حد ممکن کوچک نگه دارند تا بتوانند آن‌ها را هرچه سریع‌تر در پوشهٔ اشتراکی بارگذاری کنند. بنابراین، استخراجگرها انگیزه دارند تراکنش‌ها را کنار بگذارند؛ در حالی که دقیقاً می‌خواستید از چنین وضعیتی جلوگیری کنید. برای ایجاد انگیزه در استخراجگرها جهت گنجاندن یک تراکنش، می‌توان برای آن کارمزد تراکنش[۱۱] در نظر گرفت؛ کارمزدی که به استخراجگری می‌رسد که بلوک تاییدکنندهٔ آن تراکنش را تولید کرده است.



شکل ۱.۷: اثبات کار سامانهٔ اثبات کار جای امضاهای دیجیتال را در سرآیند بلوک‌ها می‌گیرد. اما امضاهای دیجیتال برای جلوگیری از حذف تراکنش‌ها توسط لیسا معرفی شده بودند. نگران نباشید؛ سامانهٔ اثبات کار این مسئله را نیز، البته به شیوه‌ای متفاوت، حل می‌کند. به جای آنکه بتوان تقلب لیسا را اثبات کرد، تقلب کردن را دشوار و پرهزینه می‌کنید.

در سراسر این فصل، انگیزه‌های استخراجگرها را بررسی می‌کنیم: چرا باید استخراج کنند؟ چرا پس از تأیید شدن تراکنش‌ها، آن‌ها را حذف نکنند؟ اگر یک استخراجگر بخش عمدهٔ توان چکیده‌سازی[۱۲] را در اختیار بگیرد، چه آسیبی می‌تواند وارد کند؟ دربارهٔ پویایی‌های جالب زیادی در زمینهٔ انگیزه‌های استخراجگرها می‌توان بحث کرد.

[۹] Hash – معادل فارسی: چکیده‌سازی
[۱۰] Wallet – معادل فارسی: کیف پول
[۱۱] Transaction fee – معادل فارسی: کارمزد تراکنش
[۱۲] Hash power – معادل فارسی: توان چکیده‌سازی

پوشهٔ اشتراکی چه می‌شود؟

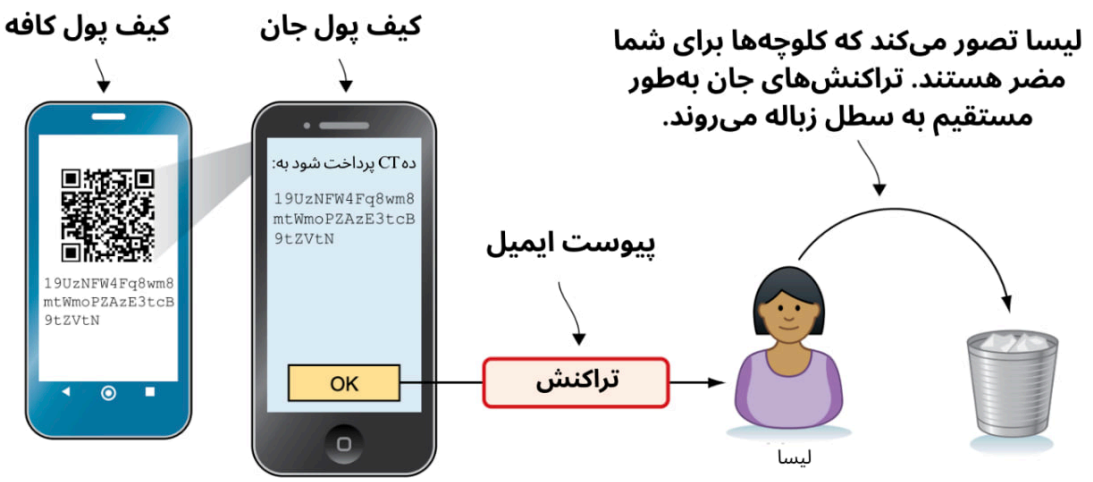
درست است؛ مدیر پوشهٔ اشتراکی نیز یک مرجع متمرکز محسوب می‌شود. او می‌تواند از افزودن برخی بلوک‌ها به آن خودداری کند؛ در نتیجه هیچ‌کس هرگز آن‌ها را نخواهد دید. این مشکل را در فصل ۸، هنگام معرفی شبکهٔ همتابه‌همتا[a]، برطرف می‌کنیم.

[a] Peer-to-Peer network – معادل فارسی: شبکهٔ همتابه‌همتا

۱.۷ تکثیر لیسا

در بخش‌های «مسائل حریم خصوصی» و «غیرمتمرکز» در فصل ۱، کمی دربارهٔ حریم خصوصی صحبت کردیم. اشاره کردم که در سامانه‌ای با یک مرجع متمرکز، آن مرجع اختیار مطلق دارد که تعیین کند چه کسی و برای چه منظوری از خدمت استفاده کند.

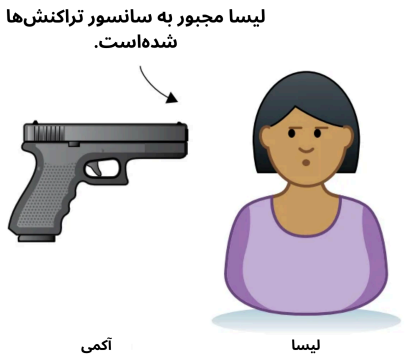
لیسا یک مرجع متمرکز است و می‌تواند هر تراکنشی را که بخواهد سانسور کند. فرض کنید لیسا به‌تازگی کتابی از یک متخصص تغذیهٔ مشهور خوانده و فهمیده است که کلوچه برای سلامتی مضر است. او احساس می‌کند باید در برابر ولع کلوچه‌خوری در شرکت اقدامی انجام دهد. بنابراین، تراکنش‌هایی را که گمان می‌کند برای خرید کلوچه انجام می‌شوند پردازش نمی‌کند؛ برای نمونه، با جست‌وجوی تراکنش‌هایی که خروجی ۱۰ CT دارند (شکل ۲.۷).



شکل ۲.۷: لیسا می‌تواند مانند یک دیکتاتور تراکنش‌ها را سانسور کند؛ برای جان کلوچه‌ای در کار نیست!

افرادی که می‌خواهند در کافه بابت یک کلوچه پول بپردازند، از دریافت خدمت محروم می‌شوند؛ زیرا پرداختشان انجام نمی‌شود. لیسا ممکن است تراکنش‌های دیگری را نیز که ارتباطی با کلوچه ندارند فیلتر کند، چون به آن‌ها مشکوک است که برای پرداخت هزینهٔ کلوچه به کار می‌روند.

احتمال دیگر سانسور این است که شرکت بیمهٔ اَکمی[۱۳]، لیسا را مجبور یا تطمیع کند تا تراکنش‌های مشکوک خرید کلوچه را کنار بگذارد؛ زیرا نمی‌خواهد مردم بر اثر چاقی بیمار شوند. یک فرد بیمار برای اَکمی به معنای زیان‌های سنگین است.



اگر چند نفر مانند لیسا داشته باشید، چه می‌شود؟ در این صورت دیگر به درست‌کاری و در دسترس بودن همیشگی یک فرد واحد وابسته نخواهید بود. فرض کنید به تام و چی نیز اجازه دهید همان کاری را انجام دهند که لیسا انجام می‌دهد. اگر کیف پول‌ها همهٔ تراکنش‌ها را برای هر سه نفر ایمیل کنند، خطر سانسور شدن یک تراکنش به‌شدت کاهش می‌یابد. اما آن‌ها چگونه می‌توانند بلوک‌ها را به‌صورتی کنترل‌شده تولید کنند تا همواره بلوک‌های متعارضی در یک ارتفاع ایجاد نکنند؟

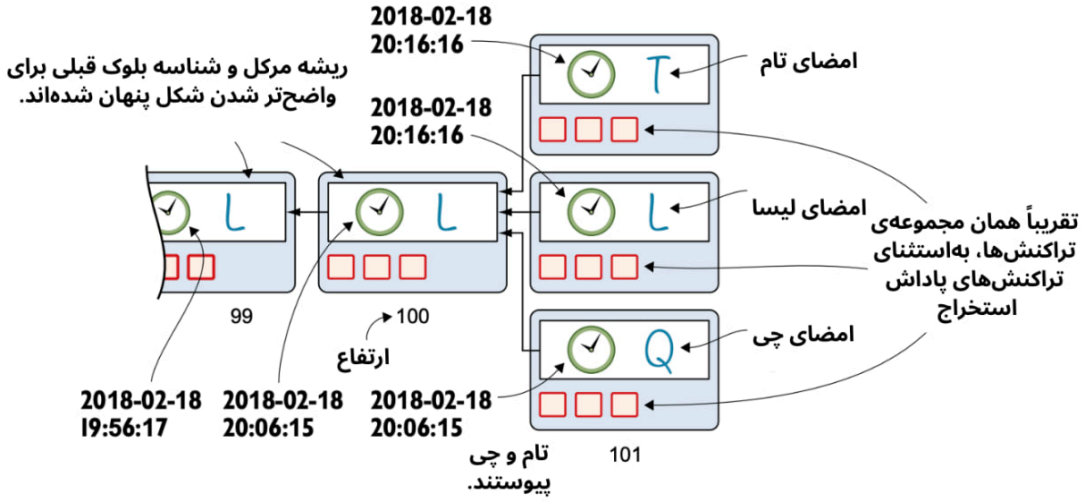
۱.۱.۷ برخورد بلوک‌ها

فرض کنید ارتفاع فعلی بلوک ۱۰۰ است. تام و چی به‌تازگی کلیدهای عمومی امضای بلوک خود را روی تابلوی اعلانات و اینترانت شرکت منتشر کرده‌اند. همهٔ کیف پول‌ها شروع می‌کنند به ارسال تراکنش‌ها برای هر سه تولیدکنندهٔ بلوک، یا استخراجگر. شکل ۳.۷ نشان می‌دهد چه اتفاقی رخ می‌دهد.

[۱۳] Acme Insurances – معادل فارسی: شرکت بیمهٔ اَکمی

استخراجگر

استخراجگر کسی است که بلوک ایجاد می‌کند. لیسا یک استخراجگر است؛ تام و چی نیز همین‌طور.



شکل ۳.۷: تام و چی درست مانند لیسا شروع به ایجاد بلوک می‌کنند و در نتیجه، برخورد بلوک‌ها رخ می‌دهد. برای خوانایی، سرآیند بلوک‌ها ساده‌سازی شده‌اند.

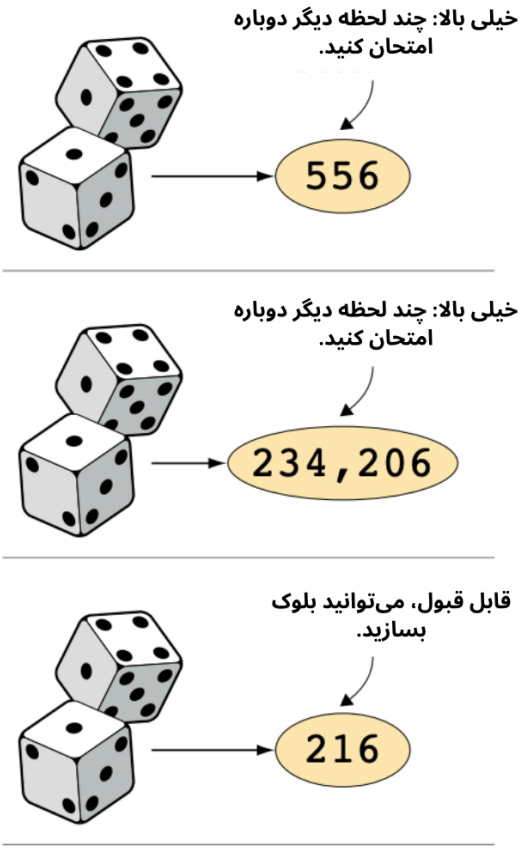
اگر هر سه نفر صرفاً همان کاری را انجام دهند که لیسا انجام می‌داد، هر ۱۰ دقیقه یک بلوک تولید می‌کنند؛ در نتیجه سه بلوک متفاوت با تقریباً تراکنش‌های یکسان به وجود می‌آید. تفاوت‌های اصلی میان این سه بلوک متعارض، تراکنش پاداش استخراج[۱۴] و امضاها هستند. پاداش استخراج بلوک‌های تام، پاداش بلوک را به نشانی توکن کلوچه[۱۵] تام پرداخت می‌کند؛ در حالی که پاداش استخراج بلوک‌های لیسا، پاداش بلوک را به نشانی توکن کلوچه لیسا می‌پردازد.

۲.۱.۷ انتخاب اعداد خوش‌شانس

برای جلوگیری از این مشکل، استخراجگرها باید به‌نحوی تصمیم بگیرند که کدام‌یک بلوک بعدی را تولید کند. آن‌ها می‌توانند نوبتی عمل کنند، اما این روش پیچیده خواهد بود؛ زیرا ممکن است رایانهٔ لیسا خراب شود یا تام به هر دلیلی از ایجاد بلوک خودداری کند. در چنین سناریویی، سامانه متوقف می‌شود.

[۱۴] Coinbase – معادل فارسی: پاداش استخراج
[۱۵] Cookie Token – معادل فارسی: توکن کلوچه

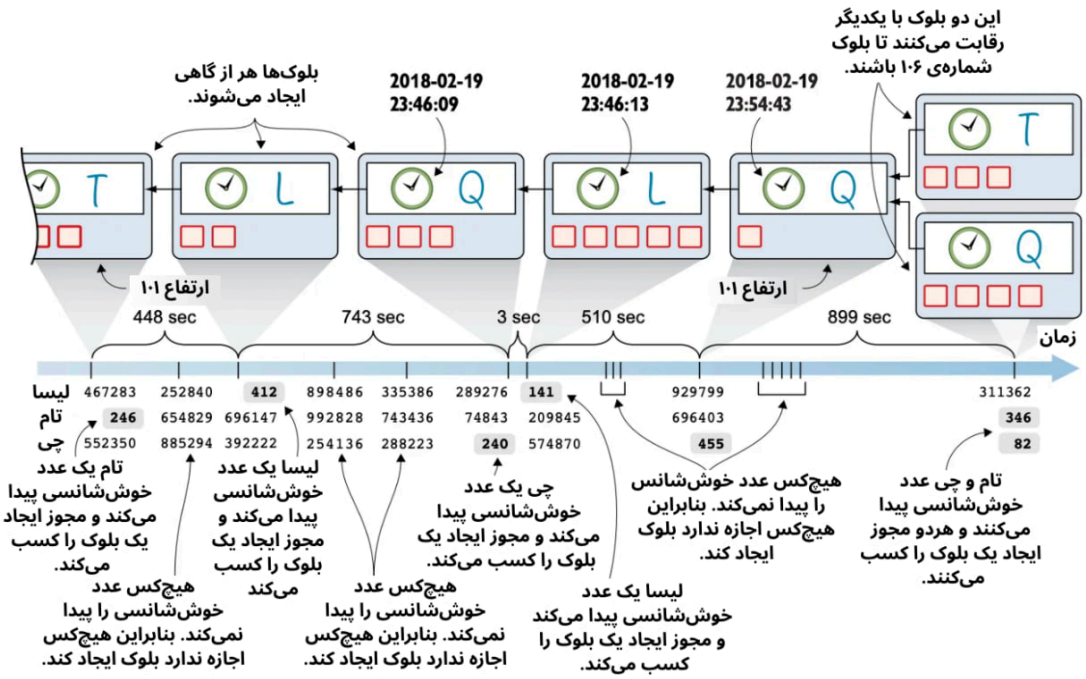
بیایید روش ساده‌انگارانهٔ دیگری را امتحان کنیم (شکل ۴.۷). هر استخراجگر در هر ثانیه، یک عدد تصادفی بین صفر تا ۹۹۹,۹۹۹ انتخاب می‌کند. اگر استخراجگری به‌طور اتفاقی عددی در بازهٔ صفر تا ۵۵۵ انتخاب کند، بلافاصله یک بلوک را امضا و منتشر می‌کند. احتمال انتخاب یک عدد خوش‌شانس[۱۶] در هر تلاش کم است: ۵۵۶ در یک میلیون، یا تقریباً یک در هر ۱۸۰۰ تلاش. استخراجگرها در هر ثانیه یک عدد انتخاب می‌کنند؛ بنابراین، به‌طور میانگین انتظار می‌رود هر استخراجگر هر ۳۰ دقیقه یک عدد خوش‌شانس انتخاب کند (۱۸۰۰ ثانیه). در نتیجه، این سه استخراجگر در مجموع به‌طور میانگین هر ۱۰ دقیقه یک بلوک تولید می‌کنند.



وقتی یک استخراجگر عدد خوش‌شانسی انتخاب می‌کند، احتمال اینکه یکی از دو استخراجگر دیگر نیز هم‌زمان عدد خوش‌شانس انتخاب کرده باشد پایین است. یعنی معمولاً فقط یک استخراجگر بلوک بعدی را تولید می‌کند.

استخراجگرها بلوک‌های خود را با نام $< last - ۸ - hexdigits - of - blockid > .dat$

[۱۶] Lucky number – معادل فارسی: عدد خوش‌شانس



شکل ۴.۷: سه استخراجگر بلوک می‌سازند. معمولاً بلوک‌ها به‌خوبی و یکی‌یکی ایجاد می‌شوند؛ اما گاهی، مانند ارتفاع ۱۰۶، برای تبدیل شدن به بلوک بعدی با هم رقابت می‌کنند.

در پوشهٔ اشتراکی ذخیره می‌کنند؛ بنابراین، چند بلوک در یک ارتفاع لازم نیست نگران نام‌گذاری فایل باشند. نمونه‌ای از نام فایل، $۹ce۳۵c۲۵.dat$ است.

سامانه به‌خوبی به کار خود ادامه می‌دهد، اما گاهی دو استخراجگر به‌طور هم‌زمان عدد خوش‌شانسی انتخاب می‌کنند. آن‌ها از انتخاب هم‌زمان استخراجگر دیگر آگاه نیستند؛ بنابراین، هر دو در یک ارتفاع بلوک تولید می‌کنند. این وضعیت «انشعاب بلاک‌چین[۱۷]» نام دارد، زیرا زنجیره به دو شاخه تقسیم می‌شود. هر دو شاخه به یک اندازه معتبرند؛ پس کدام‌یک «درست» است؟ کدام استخراجگر برنده می‌شود و پاداش ۵۰ CT بلوک را دریافت می‌کند؟

هنوز برنده مشخص نیست. این به استخراجگرها بستگی دارد که تصمیم بگیرند بلوک‌های بعدی خود را روی کدام شاخه گسترش دهند. در شکل ۴.۷، تام و چی هر دو در ارتفاع ۱۰۶ یک بلوک ایجاد کرده‌اند. استخراجگرهای مختلف احتمالاً چنین فکر می‌کنند:

تام: «شاخهٔ خودم را ادامه می‌دهم؛ چون اگر بلوک بعدی را برنده شوم، پاداش دو بلوک را می‌گیرم.»

[۱۷] Blockchain split – معادل فارسی: انشعاب زنجیرهٔ بلوکی

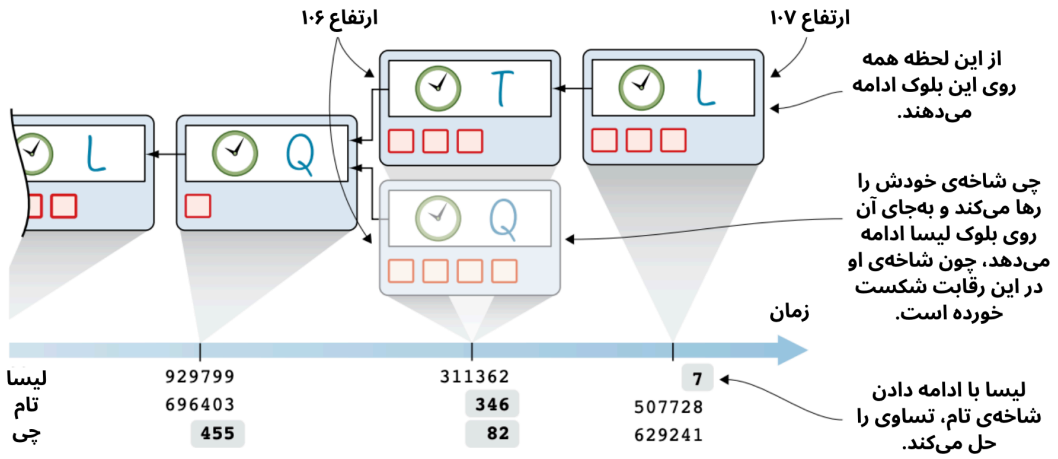
چی: «شاخهٔ خودم را ادامه می‌دهم؛ چون اگر بلوک بعدی را برنده شوم، پاداش دو بلوک را می‌گیرم.»

لیسا: «یکی از این دو بلوک را ادامه می‌دهم؛ برایم فرقی ندارد کدام. فقط نخستین بلوکی را که با موفقیت اعتبارسنجی کردم انتخاب می‌کنم: بلوک تام. ممکن است این بلوک‌ها دقیقاً هم‌زمان در پوشهٔ اشتراکی قرار نگرفته باشند؛ بنابراین منطقی است نخستین بلوک معتبری را که دیده‌ام ادامه دهم.»

وقتی استخراجگرها یک بلوک در ارتفاع ۱۰۶ را برای ادامه‌دادن انتخاب می‌کنند، بلوک جدیدی در ارتفاع ۱۰۷ می‌سازند و دوباره شروع به انتخاب اعداد می‌کنند. با فرض درست‌کار بودن همه، چند نتیجهٔ ممکن وجود دارد: حل فوری، حل با تأخیر، یا انشعاب یک انشعاب.

حل فوری

در ساده‌ترین و رایج‌ترین حالت، دقیقاً یک استخراجگر نخستین کسی است که عدد خوش‌شانسی انتخاب می‌کند. این بار لیسا خوش‌شانس است (شکل ۵.۷).



شکل ۵.۷: حل فوری: لیسا یک عدد خوش‌شانس انتخاب می‌کند.

لیسا بلوک تام را ادامه داده است؛ بنابراین شاخه‌ای که تام و لیسا روی آن کار می‌کردند، یک بلوک بلندتر می‌شود. یکی از قواعد این بلاک‌چین آن است که طولانی‌ترین زنجیره، زنجیرهٔ درست محسوب می‌شود. این موضوع در ادامهٔ فصل تغییر خواهد کرد، اما فعلاً از طولانی‌ترین زنجیره پیروی می‌کنیم.

چی که می‌کوشید شاخهٔ خودش را ادامه دهد، متوجه می‌شود شاخهٔ دیگر به‌تازگی بلندتر شده است؛ زیرا لیسا برای آن شاخه بلوکی منتشر کرده است. چی می‌داند که دیگران از شاخهٔ بلندتر پیروی خواهند کرد. اگر او در شاخهٔ کوتاه خود بماند، احتمالاً هرگز نمی‌تواند به شاخهٔ دیگر برسد و از آن بلندتر شود. بهتر است شاخهٔ کوتاهش را رها کند و به شاخهٔ بلندتر بپیوندد. اکنون همه دوباره روی یک شاخه کار می‌کنند و تساوی برطرف شده است.

وقتی چی به شاخهٔ جدید منتقل می‌شود، همهٔ تراکنش‌های شاخهٔ قدیمی خود را که از پیش در شاخهٔ جدید نیستند، در وضعیت «در انتظار» قرار می‌دهد. این تراکنش‌ها برای گنجانده‌شدن در بلوک‌های آیندهٔ شاخهٔ جدید در دسترس خواهند بود. گره‌ها مجموعه‌ای از تراکنش‌های در انتظار را نگهداری می‌کنند که معمولاً «استخر حافظه» یا ممپول[۱۸] نامیده می‌شود. قراردادن یک تراکنش در وضعیت در انتظار یعنی افزودن آن به ممپول.

مجموعهٔ UTXO[۱۹] مجموعهٔ خروجی‌های خرج‌نشدهٔ تراکنش از یک زنجیرهٔ واحد ساخته می‌شود و نمی‌توان آن را به‌طور هم‌زمان از چند شاخه ایجاد کرد. گره‌های کامل باید انتخاب کنند که از کدام شاخه پیروی کنند.

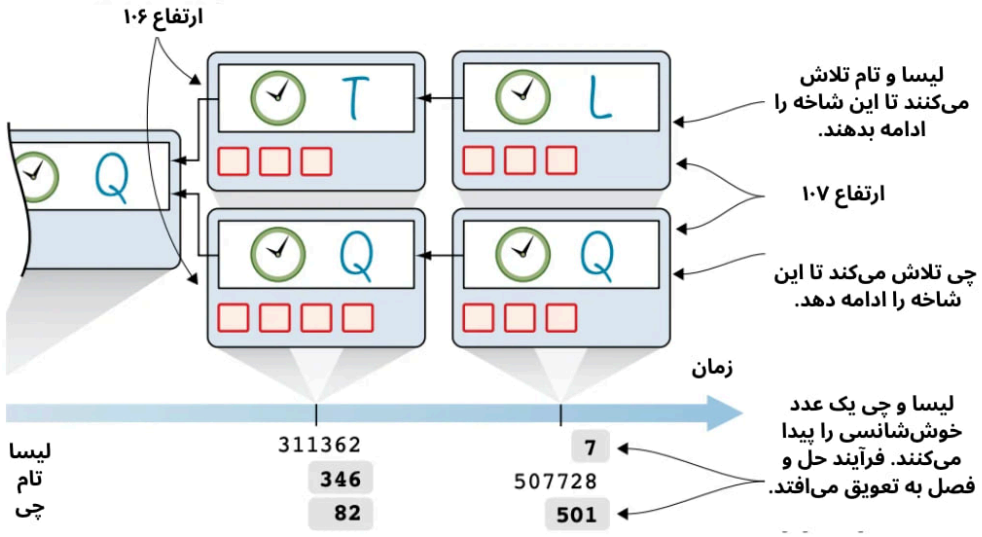
از آنجا که چی شاخهٔ خود را رها کرده است، پاداش بلوک خود را نیز رها می‌کند. بلوک او هرگز بخشی از طولانی‌ترین زنجیره نخواهد شد؛ بنابراین هرگز نمی‌تواند پاداش بلوک موجود در آن را خرج کند. فقط بلوک‌های واقع در طولانی‌ترین زنجیره بر مجموعهٔ UTXO اثر می‌گذارند.

حل با تأخیر

اما اگر لیسا و چی به‌طور اتفاقی در یک ثانیه عدد خوش‌شانسی انتخاب کنند، چه اتفاقی می‌افتد؟ (شکل ۶.۷) در این صورت، هر دو شاخه هرکدام به اندازهٔ یک بلوک گسترش می‌یابند. هنوز نمی‌دانید کدام شاخه درست است. استخراجگرها دوباره طرف خود را انتخاب می‌کنند و می‌کوشند شاخهٔ منتخب خود را ادامه دهند.

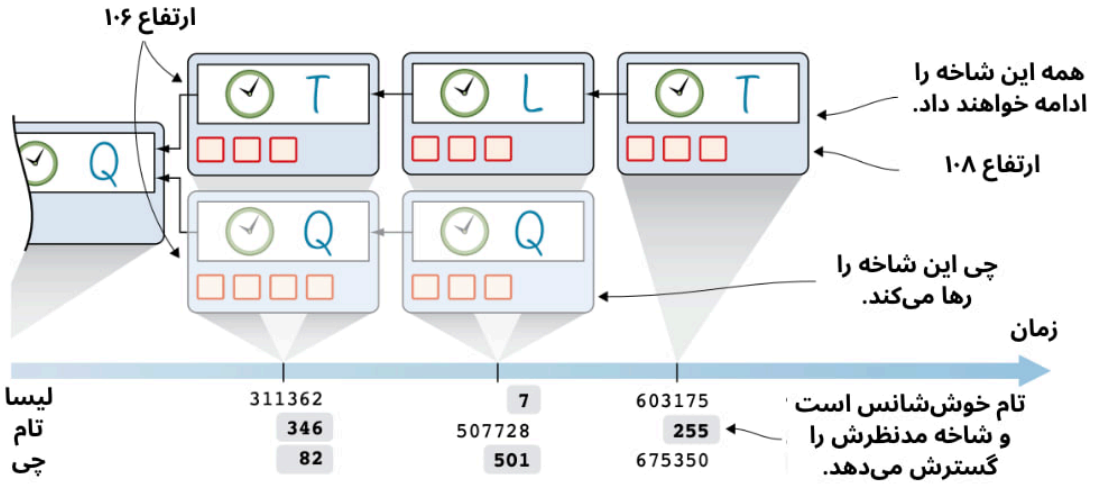
فرض کنید تام نفر بعدی است که عدد خوش‌شانسی انتخاب می‌کند. او بلوک بعدی را روی شاخهٔ خود می‌سازد؛ شاخه‌ای که اکنون سه بلوک طول دارد. این شاخه از شاخهٔ

[۱۸] Mempool – معادل فارسی: استخر حافظهٔ تراکنش‌ها
[۱۹] Unspent Transaction Output (UTXO) set – معادل فارسی: مجموعهٔ خروجی‌های خرج‌نشدهٔ تراکنش



شکل ۶.۷: لیسا و چی به‌طور هم‌زمان یک عدد خوش‌شانس انتخاب می‌کنند. وضعیت هنوز حل نشده است.

دیگر، که فقط دو بلوک دارد، بلندتر می‌شود (شکل ۷.۷).

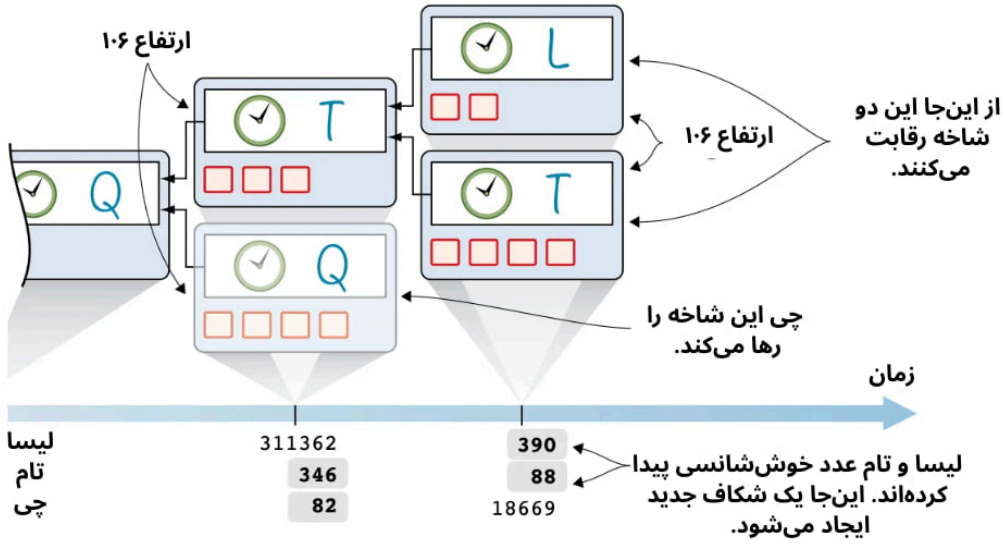


شکل ۷.۷: تام استخراجگر خوش‌شانس بعدی است و می‌تواند شاخهٔ «خودش» را گسترش دهد؛ شاخه‌ای که اکنون به طولانی‌ترین شاخه تبدیل می‌شود.

همهٔ استخراجگرها با تغییر مسیر به شاخهٔ تام و ادامه‌دادن کار از آن نقطه، این موضوع را می‌پذیرند. سرانجام یک شاخهٔ برنده دارید. بار دیگر، چی بازندهٔ این رقابت است.

انشعاب یک انشعاب

حالا فرض کنید تام و لیسا هر دو در یک زمان عدد خوش‌شانسی انتخاب کنند. در این حالت، هر دو شاخهٔ تام را گسترش می‌دهند. نتیجه، انشعابی از یک انشعاب خواهد بود (شکل ۸.۷).



شکل ۸.۷: یکی از شاخه‌ها یک انشعاب دیگر را تجربه می‌کند. این انشعاب جدید نیز مانند انشعاب قبلی حل می‌شود.

اکنون سه شاخه دارید. شاخهٔ چی احتمالاً کنار گذاشته می‌شود، زیرا از دو شاخهٔ جدید، یعنی شاخهٔ لیسا و شاخهٔ تام، کوتاه‌تر است. این رقابت تازه نیز به همان روشی حل می‌شود که انشعاب نخست حل شد:

بلافاصله، با بلوک بعدی؛

با تأخیر، زیرا دو بلوک به‌طور هم‌زمان، یکی روی هر شاخه، پدیدار می‌شوند؛

یا هنگامی که انشعاب جدیدی در یکی از این دو شاخه ایجاد شود.

۳.۱.۷ احتمال انشعاب‌ها

در نهایت، یکی از شاخه‌های یک انشعاب برنده می‌شود. با افزایش طول شاخه، احتمال رخ‌دادن دو شاخه با طول X به‌سرعت کاهش می‌یابد:

جدول ۱.۷: احتمال رخ‌دادن انشعاب‌های هم‌زمان با طول‌های مختلف.

طول شاخه	احتمال	تقریباً هر چند وقت یک‌بار رخ می‌دهد
۱	$۵/۶ \times ۱۰^{-۴}$	۲ هفته
۲	$۲/۱ \times ۱۰^{-۷}$	۹۰ سال
۳	$۷/۶ \times ۱۰^{-۱۱}$	۲۵۰۰۰۰ سال
۴	$۲/۸ \times ۱۰^{-۱۴}$	۷۰۰۰۰۰۰۰۰ سال

نمادگذاری علمی

عبارت $X\mathrm{e}{-}Y$ شکل کوتاه‌شدهٔ $X \times ۱۰^{-Y}$ است. برای مثال، ۵/۶e−۴ برابر با ۰/۰۰۰۵۶ است.

انشعاب با طول شاخهٔ ۱، رخدادی نسبتاً محتمل است؛ اما شاخه‌ای با طول ۲ احتمالاً در طول عمر لیسا رخ نمی‌دهد؛ او ۴۵ سال دارد. با این حال، انشعاب‌ها هرقدر هم طول بکشند، سرانجام با تعیین یک برنده حل می‌شوند.

این سازوکار مناسب به نظر می‌رسد، اما مشکلاتی دارد:

می‌توان با اعداد خوش‌شانس تقلب کرد. نمی‌توانید اثبات کنید که واقعاً یک عدد خوش‌شانس را به‌صورت صادقانه انتخاب کرده‌اید.

هر استخراجگر جدید، سامانه را در برابر سانسور مقاوم‌تر، اما در برابر سرقت کلید خصوصی[۲۰] آسیب‌پذیرتر می‌کند. هرچه رایانه‌های بیشتری دارای کلید خصوصی باشند، احتمال سرقت یک کلید بیشتر می‌شود. کلید خصوصی سرقت‌شده برای امضای بلوک به سارق اجازه می‌دهد با تقلب در انتخاب اعداد خوش‌شانس، بلوک بسازد و پاداش‌ها را برای خود بردارد.

با افزوده‌شدن هر استخراجگر، خطر تقلب یک استخراجگر در انتخاب اعداد خوش‌شانس افزایش می‌یابد.

[۲۰] Private key – معادل فارسی: کلید خصوصی

انشعاب‌ها

انشعاب‌ها در بیت‌کوین کمتر از ماهی یک بار رخ می‌دهند و با گذر زمان، به دلیل کاراترشدن سازوکارهای اعتبارسنجی و انتقال داده، روند کاهشی دارند.

نمی‌توان استخراجگرهای جدید را صرفاً به سامانه اضافه کرد. با افزایش تعداد استخراجگرها، باید آستانهٔ عدد خوش‌شانس را پایین آورد تا میانگین ۱۰ دقیقه برای هر بلوک و نرخ انتشار پول در سطح مطلوب حفظ شود.

روشن است که این سامانه نمی‌تواند تعداد استخراجگرها را فراتر از گروه کنترل‌شده‌ای از مشارکت‌کنندگان کاملاً مورداعتماد افزایش دهد. با آغاز تقلب استخراجگرها، سیلی از بلوک‌ها ایجاد می‌شود؛ اما نمی‌توانید ثابت کنید که تقلب می‌کنند. ممکن است واقعاً فقط بسیار، بسیار خوش‌شانس باشند.

کجا بودیم؟

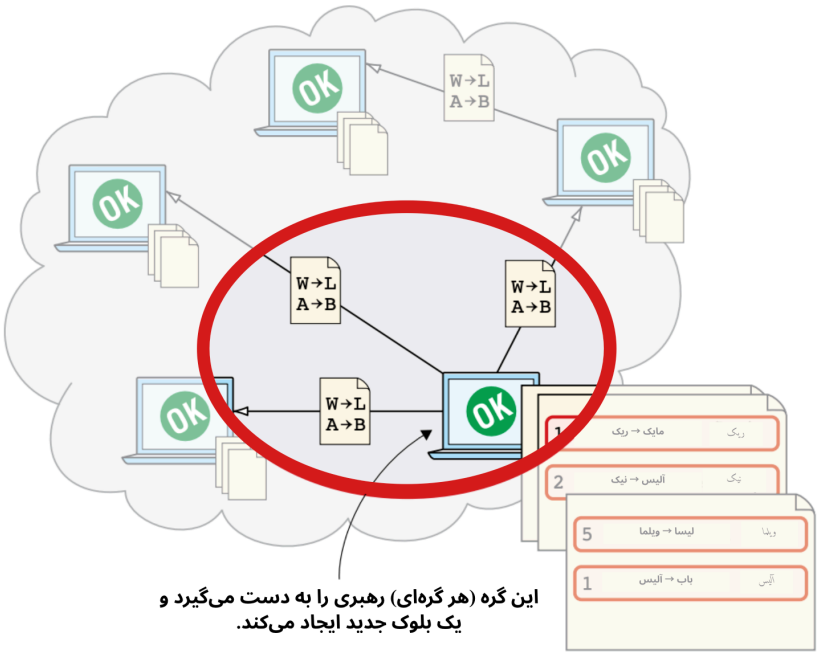
این فصل دربارهٔ اثبات کار است. هنوز این اصطلاح را به‌درستی معرفی نکرده‌ام، اما در بخش بعدی این کار را انجام می‌دهم.

در مرور کلی بیت‌کوین، در بخش «گام ۳: بلاک‌چین» از فصل ۱، دیدید که یک استخراجگر پیش‌قدم می‌شود و تصمیم می‌گیرد کدام تراکنش‌ها و با چه ترتیبی وارد بلوک بعدی شوند. بیت‌کوین برای تعیین اینکه چه کسی این نقش را بر عهده بگیرد، از اثبات کار استفاده می‌کند (شکل ۹.۷).

اثبات کار به شما اجازه می‌دهد بدون استفاده از یک مرجع متمرکز، به‌طور تصادفی یک رهبر را از میان همهٔ استخراجگرها انتخاب کنید. به این فصل با دقت توجه کنید.

این موضوع، جوهرهٔ بیت‌کوین است و همان چیزی است که بیت‌کوین را واقعاً غیرمتمرکز می‌کند. ما سامانهٔ غیرمتمرکز می‌خواهیم، زیرا چنین سامانه‌ای در برابر سانسور مقاوم است. اگر سامانه دارای مرجع مرکزی باشد، تراکنش‌ها می‌توانند سانسور شوند.

تکثیر لیسا نخستین گام به سوی غیرمتمرکزسازی بود، اما کامل نیست؛ زیرا به استخراجگرها اعتماد می‌کنید که اعداد خوش‌شانس را صادقانه انتخاب کنند.



شکل ۹.۷: اثبات کار روشی برای انتخاب رهبر، بدون وجود رهبر است.

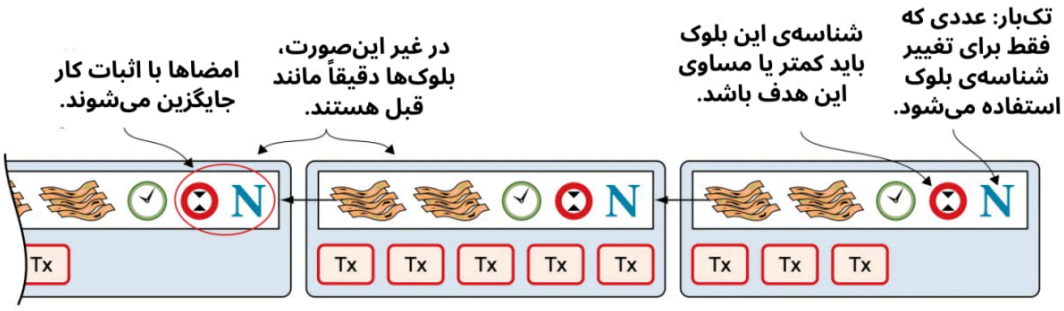
۲.۷ واداشتن ماینرها به انتخاب صادقانهٔ اعداد خوش‌شانس

اگر بتوانید استخراجگرها را وادار کنید که در انتخاب اعداد خوش‌شانس تقلب نکنند، چه می‌شود؟ مشخص می‌شود که این کار شدنی است. می‌توانید آن‌ها را وادار کنید با رایانه‌های خود حجم عظیمی از محاسبات را انجام دهند و سپس ثابت کنند که این کار را انجام داده‌اند. می‌توانید آن‌قدر کار محاسباتی از آن‌ها بخواهید که تولید هر بلوک، برای هر یک از این سه استخراجگر، به‌طور میانگین حدود ۳۰ دقیقه زمان ببرد. در نتیجه، مانند قبل، فاصلهٔ زمانی میان بلوک‌ها به ۱۰ دقیقه می‌رسد.

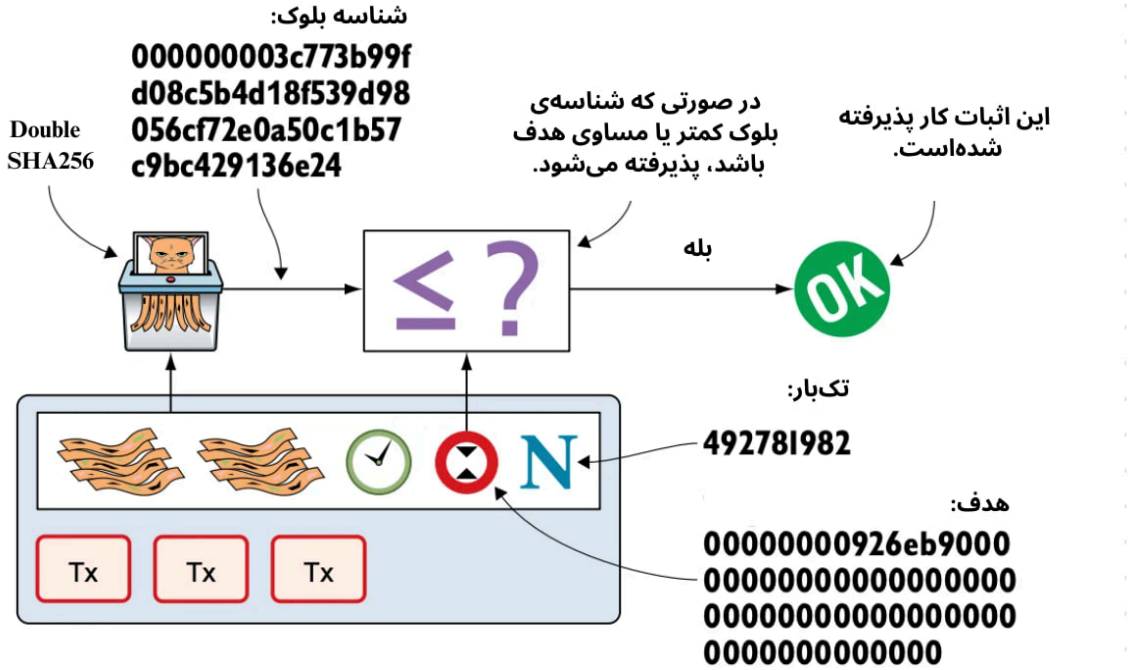
ترفند این است که امضاهای دیجیتال موجود در سرآیند بلوک را با اثبات کار جایگزین کنیم (شکل ۱۰.۷). فرض کنید چی به‌تازگی بلوکی منتشر کرده و گرهٔ کامل کافه می‌خواهد اعتبار آن را بررسی کند. افزون بر بررسی موارد معمول، مانند تراکنش‌ها و ریشهٔ مرکل[۲۱]، گرهٔ کامل باید بررسی کند که بلوک چی شامل اثبات کار معتبر باشد. اثبات کار زمانی معتبر است که چکیده سرآیند بلوک، یعنی شناسهٔ بلوک[۲۲]، کوچک‌تر یا

[۲۱] Merkle root – معادل فارسی: ریشهٔ مرکل
[۲۲] Block ID – معادل فارسی: شناسهٔ بلوک

مساوی یک هدف[۲۳] موردتوافق باشد که در سرآیند بلوک نوشته شده است؛ همان‌گونه که شکل ۱۱.۷ نشان می‌دهد.



شکل ۱۰.۷: امضاهای بلوک با اثبات کار جایگزین می‌شوند.

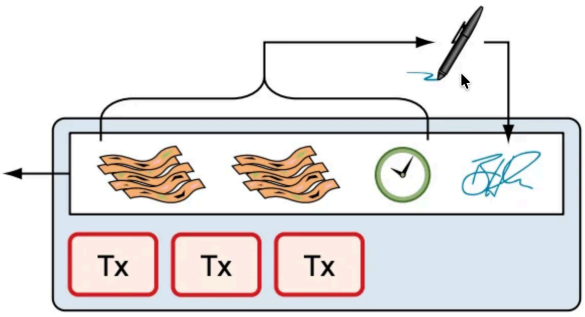


شکل ۱۱.۷: شناسهٔ بلوک باید کوچک‌تر یا مساوی هدف موجود در سرآیند باشد؛ در غیر این صورت، بلوک نامعتبر است.

---

[۲۳] Target – معادل فارسی: هدف

سبک قدیمی بلوک‌ها



تک‌بار[۲۴] در این سرآیند بلوک برابر با ۴۹۲۷۸۱۹۸۲ است. چی این مقدار را با آزمون‌وخطا انتخاب می‌کند. بخش بعدی توضیح می‌دهد که این فرایند چگونه انجام می‌شود.

برای تعیین معتبر بودن اثبات کار یک بلوک، شناسهٔ ۲۵۶بیتی بلوک را با هدف ۲۵۶بیتی نوشته‌شده در سرآیند بلوک مقایسه کنید. در شکل ۱۱.۷، شناسهٔ بلوک و هدف به‌صورت زیرند:

```
block id:  000000003c773b99fd08c5b4d18f539d98056cf72e0a50c1b57c9bc429136e24

target:  00000000926eb900000000000000000000000000000000000000000000000000
```

در این مثال، شناسهٔ بلوک با ۰۰۰۰۰۰۰۰۳ آغاز می‌شود، در حالی که هدف با ۰۰۰۰۰۰۰۰۹ شروع می‌شود. شناسهٔ بلوک از هدف کوچک‌تر است؛ بنابراین اثبات کار این بلوک معتبر است.

هدف، عددی است که همهٔ گره‌های کامل و استخراجگرها بر سر آن توافق دارند. این هدف هر از گاهی و بر اساس قواعد مشترک تغییر می‌کند. چنین تغییری «تنظیم مجدد هدف[۲۵]» نام دارد که در بخشی دیگر توضیح داده خواهد شد. فعلاً می‌توانید آن را عدد ثابتی در نظر بگیرید که باید در سرآیند بلوک قرار بگیرد.

۱.۲.۷ تولید اثبات کار معتبر

برای ایجاد یک بلوک جدید، استخراجگر باید پیش از معتبر تلقی‌شدن بلوک، یک اثبات کار معتبر برای آن تولید کند. برای تولید اثبات کار معتبر، استخراجگر باید چکیده

[۲۴] Nonce – معادل فارسی: تک‌بار
[۲۵] Retarget – معادل فارسی: تنظیم مجدد هدف

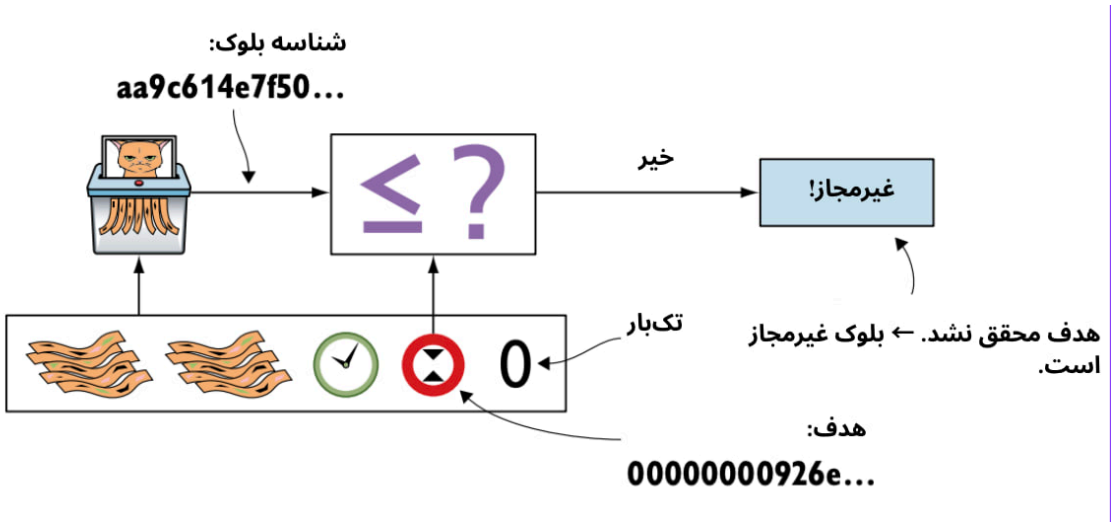
سرآیند بلوکی بسازد که کوچک‌تر یا مساوی هدف درج‌شده در سرآیند باشد.

اهداف در بیت‌کوین

هدف در سرآیند بلوک به‌صورت ۴ بایت، یعنی ABCD، ثبت می‌شود؛ اما هدف ۳۲بایتی به شکل BCD × $۲^{۸\times(A-۳)}$ محاسبه می‌شود. به بیان دیگر، پس از BCD، به تعداد ۳A- بایت صفر قرار می‌گیرد. این قالب نامعمول به این دلیل است که باید دامنهٔ گسترده‌ای از اهداف، از ۱ تا $۲^{۲۵۶}$، را تنها با ۳۲ بیت نمایش دهیم. هدف در بلوک چی به‌صورت ۹eb۹۲۶c۱ ثبت شده است؛ یعنی ۹eb۹۲۶ که پس از آن ۲۵ بایت صفر قرار گرفته است.

شناسهٔ بلوک، حاصل $DoubleSHA-۲۵۶$ بر سرآیند بلوک است. همان‌طور که در فصل ۲ آموختید، تنها راه یافتن پیش‌تصویر[۲۶] برای یک تابع چکیده رمزنگاری، آزمودن مکرر ورودی‌های مختلف تا یافتن یک پاسخ مناسب است. اینجا نیز همین‌طور است؛ استخراجگر باید سرآیندهای مختلفی را امتحان کند تا سرانجام به سرآیندی برسد که چکیده آن کوچک‌تر یا مساوی هدف باشد.

بیایید به زمانی برگردیم که چی بلوک خود را ایجاد می‌کرد. او یک بلوک می‌سازد، هدف را روی e...۰۰۰۰۰۰۰۰۰۹۲۶ قرار می‌دهد و تک‌بار را صفر می‌گذارد. سپس بررسی می‌کند که آیا اثبات کار معتبر است یا خیر (شکل ۱۲.۷).



شکل ۱۲.۷: چی با بررسی اثبات کار، آزمایش می‌کند که بلوکش معتبر است یا نه.

[۲۶] Pre-image – معادل فارسی: پیش‌تصویر

او شناسهٔ بلوک را با DoubleSHA – محاسبه می‌کند. در این حالت، شناسهٔ بلوک ۵۰f۷e۶۱۴c۹aa... است. این عدد از هدف بزرگ‌تر است:

```
block id: aa9c614e7f5064ef11eedc51856cc7bfcdf71a1f2d319e56d4cc65bda939be79

target: 00000000926eb900000000000000000000000000000000000000000000000000
```

قاعده این است که برای معتبر بودن اثبات کار، شناسهٔ بلوک باید کوچک‌تر یا مساوی هدف باشد. چی به‌کلی ناموفق می‌شود.

اینجاست که تک‌بار وارد عمل می‌شود. تک‌بار صرفاً عددی بی‌معناست و می‌تواند هر مقداری داشته باشد. چی در ابتدا تک‌بار را صفر قرار داد، اما می‌توانست به همان اندازه مقدار ۱۲۳ یا ۹۲۱۷۸۲۳۷ را انتخاب کند. تک‌بار باعث می‌شود تغییری در بلوک ایجاد شود که بر شناسهٔ بلوک اثر دارد، بی‌آنکه داده‌های واقعی مانند تراکنش‌ها یا شناسهٔ بلوک پیشین تغییر کنند.

چی اکنون دوباره تلاش می‌کند تا اثبات کار معتبری بسازد. او تک‌بار را از صفر به یک افزایش می‌دهد و دوباره اعتبار را می‌آزماید (شکل ۱۳.۷). هنگامی که چی با افزایش تک‌بار سرآیند بلوک را تغییر می‌دهد، شناسهٔ بلوک نیز تغییر می‌کند؛ هر تغییر بسیار کوچکی در سرآیند، شناسهٔ بلوکی کاملاً متفاوت ایجاد می‌کند.

تک‌بار

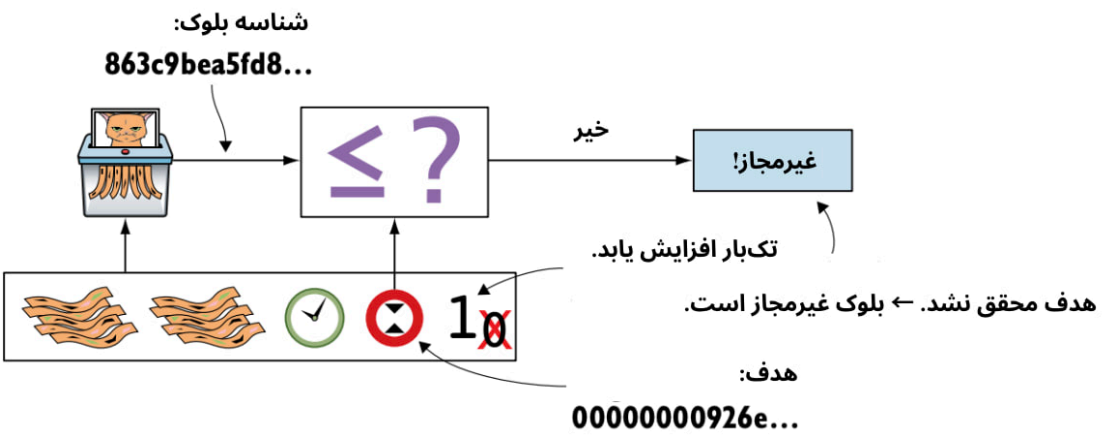
تک‌بار یک عدد ۳۲بیتی است؛ بنابراین فقط $۲^{۳۲}$، یعنی ۴۲۹۴۹۶۷۲۹۶ مقدار تک‌بار متفاوت برای انتخاب وجود دارد.

این همان ویژگی‌ای است که در بخش «هش‌های رمزنگاری» از فصل ۲، هنگام تغییر تصویر گربه، مشاهده کردیم (شکل ۱۴.۷).

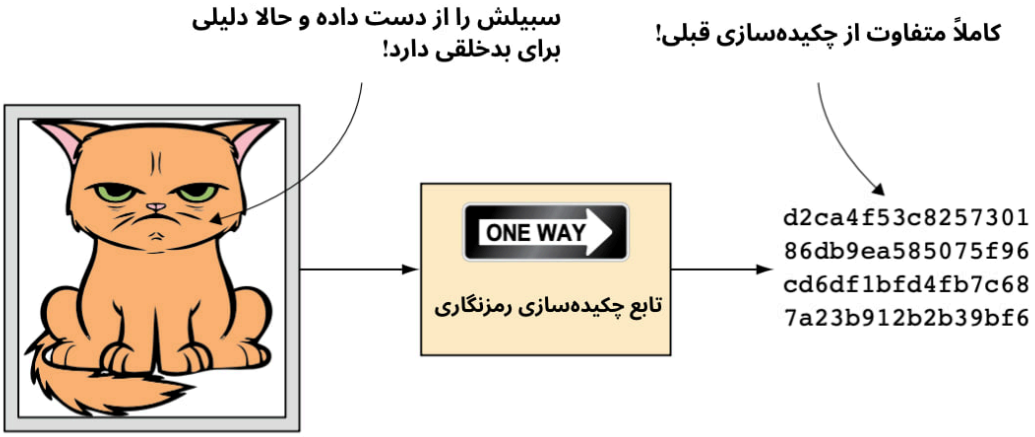
شناسهٔ بلوک جدید ...۸۶۳c۹bea۵fd۸ است. این مقدار نیز از هدف بزرگ‌تر است و چی بار دیگر شکست می‌خورد. متأسفانه راه دیگری وجود ندارد؛ چی باید دوباره تلاش کند. او تک‌بار را از ۱ به ۲ افزایش می‌دهد و بار دیگر آن را می‌آزماید (شکل ۱۵.۷).

نتیجه همان است: شکستی کامل. شناسهٔ بلوک این بار aa...۵db۲۲ce۰۰۵ بود که همچنان از هدف بزرگ‌تر است.

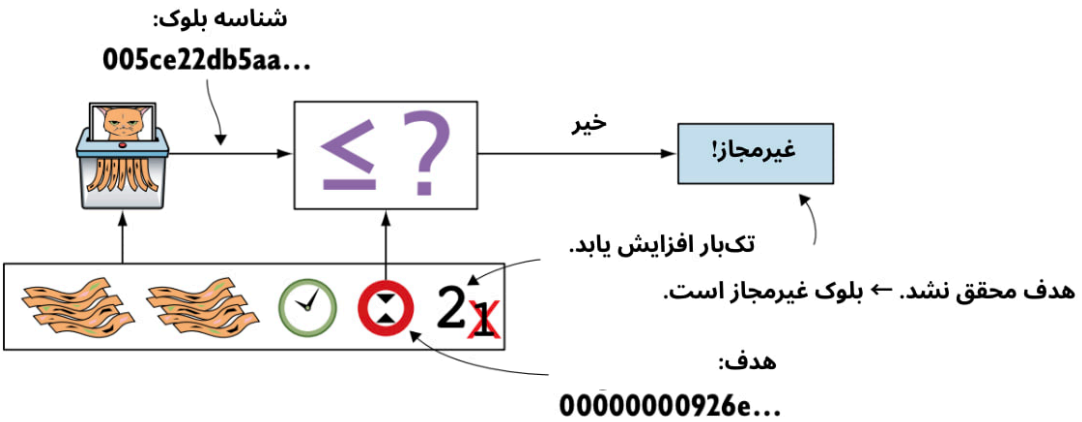
او این کار را بارها و بارها تکرار می‌کند. برای نمونه، شکل ۱۶.۷ تلاش ۲۲۷،۲۹۹،۱۲۵ام او را نشان می‌دهد. پاسخ نزدیک بود، اما نزدیک‌بودن کمکی



شکل ۱۳.۷: چی تک‌بار را افزایش می‌دهد و دومین تلاش خود را برای یافتن اثبات کار معتبر انجام می‌دهد. این تلاش نیز ناموفق است.

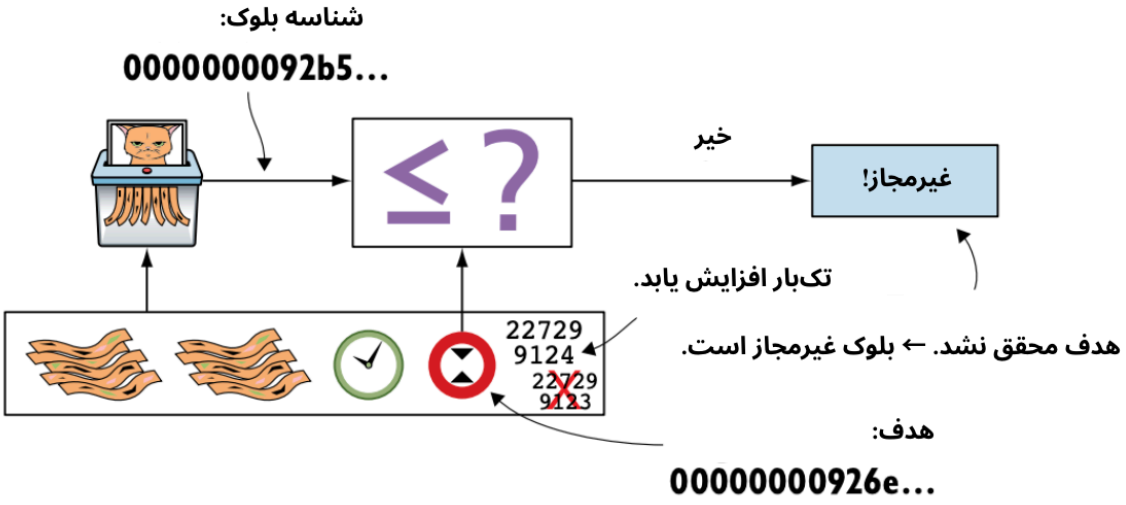


شکل ۱۴.۷: تغییر ورودی یک تابع چکیده‌سازی رمزنگاری، خروجی کاملاً متفاوتی ایجاد می‌کند.

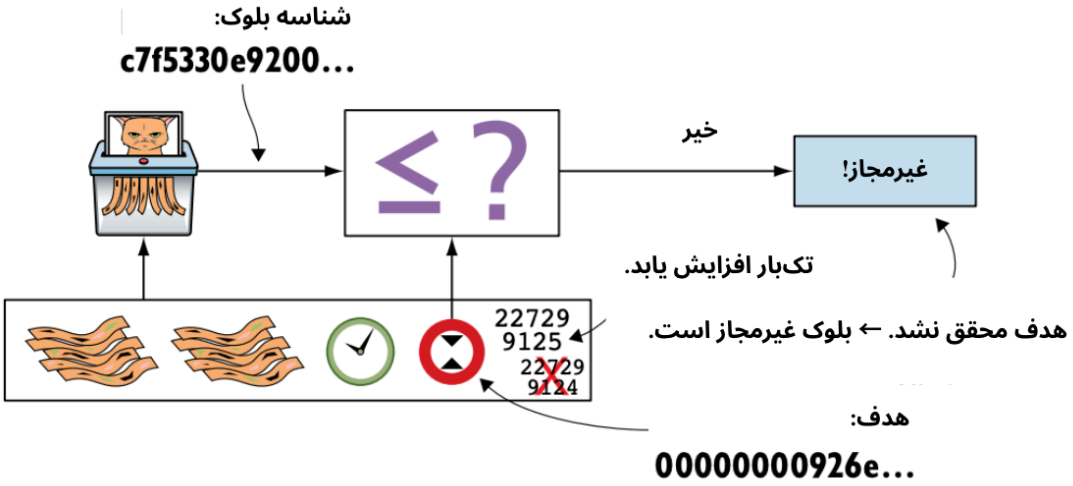


شکل ۱۵.۷: سومین تلاش چی برای یافتن اثبات کار معتبر؛ او باز هم موفق نمی‌شود.

نمی‌کند. او باید به تلاش ادامه دهد (شکل ۱۷.۷). و سرانجام، به نتیجه‌ای می‌رسد که در شکل ۱۸.۷ نشان داده شده است.



شکل ۱۶.۷: تلاش چی با تک‌بار ۲۲۷,۲۹۹,۱۲۴؛ نزدیک بود، اما کافی نبود.

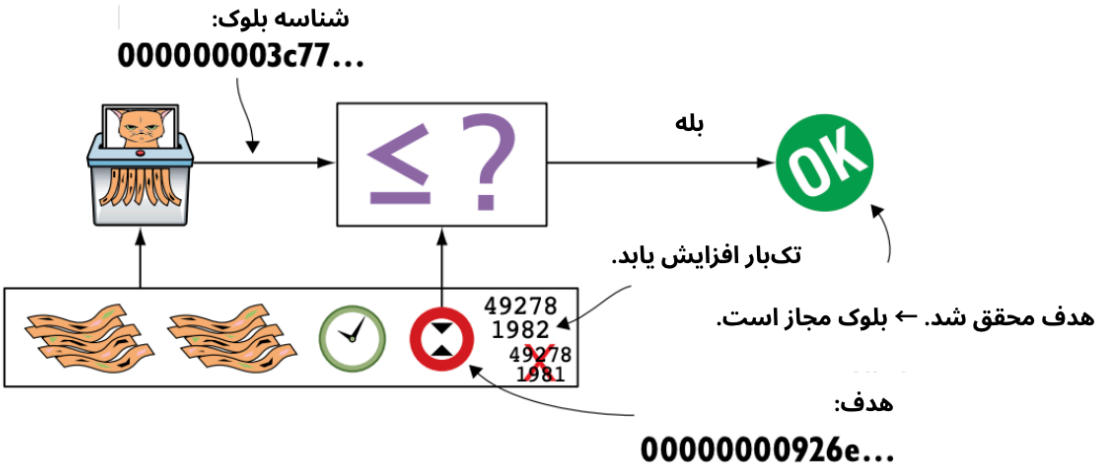


شکل ۱۷.۷: چی به کار خود ادامه می‌دهد.

تک‌بار ۴۹۲۷۸۱۹۸۲ شناسهٔ بلوک ۰۰۰۰۰۰۰۰۰۳c۷۷... را ایجاد می‌کند. چی آن را با هدف مقایسه می‌کند:

```
block id:  000000003c773b99fd08c5b4d18f539d98056cf72e0a50c1b57c9bc429136e24

target:  00000000926eb900000000000000000000000000000000000000000000000000
```



شکل ۱۸.۷: تک‌بار ۴۹۲،۷۸۱،۹۸۲ یک تک‌بار برنده است.

شناسهٔ این بلوک از هدف کوچک‌تر است. چی حجم بسیار زیادی کار انجام داده تا تک‌باری بیابد که شناسهٔ بلوک حاصل از آن کوچک‌تر از هدف باشد. او بلوکی با اثبات کار معتبر ساخته است؛ بنابراین اکنون آن را در پوشهٔ اشتراکی منتشر می‌کند.

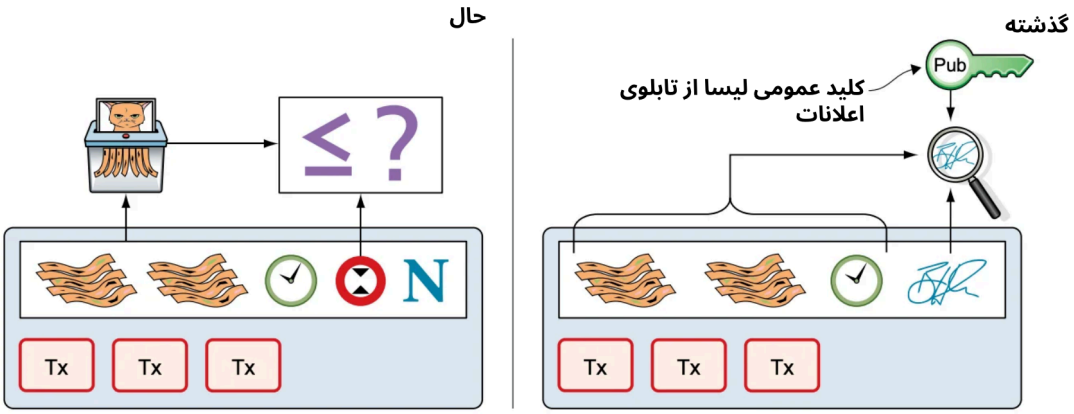
باید توجه داشت که همهٔ استخراجگرها بلوک‌های منحصربه‌فرد خود را می‌سازند. برای مثال، تام هم‌زمان با چی و لیسا روی بلوک خودش کار می‌کند، اما مجموعهٔ تراکنش‌های او با چی تفاوت دارد؛ زیرا تراکنش پاداش استخراج تام پاداش بلوک را به خودش می‌پردازد، در حالی که تراکنش پاداش استخراج چی پاداش را به چی می‌پردازد. این تفاوت باعث می‌شود ریشه‌های مرکل موجود در سرآیند بلوک‌های آن‌ها متفاوت باشد. اگر تام تک‌بار برندهٔ چی، یعنی ۴۹۲،۷۸۱،۹۸۲، را در بلوک خود قرار دهد، احتمالاً به هدف نمی‌رسد. مهر زمانی[۲۷] یا فهرست انتخاب‌شدهٔ تراکنش‌ها نیز احتمالاً از دیگر تفاوت‌های میان بلوک‌های آن‌ها هستند.

۲.۲.۷ چرا این روش مفید است؟

هر کسی می‌تواند بلوک را از پوشهٔ اشتراکی بردارد و بررسی کند که قاعده رعایت شده است: شناسهٔ بلوک کوچک‌تر یا مساوی هدف موردتوافق است. اعتبارسنجی بلوک اکنون اندکی با گذشته تفاوت دارد (شکل ۱۹.۷).

تفاوت این روش با اعتبارسنجی یک بلوک دارای امضای دیجیتال در این است که

[۲۷] Timestamp – معادل فارسی: مهر زمانی



شکل ۱۹.۷: اعتبارسنجی بلوک تغییر کرده است. اعتبارسنج دیگر به چیزی خارج از خود بلوک نیاز ندارد.

گرهٔ کامل، به‌جای بررسی امضای دیجیتال معتبر، بررسی می‌کند که تولیدکنندهٔ بلوک اثبات کار معتبری ارائه کرده باشد.

> **بلوک‌ها خودبسنده‌اند**
> برای اعتبارسنجی بلوک، به هیچ چیزی خارج از بلاک‌چین نیاز ندارید.

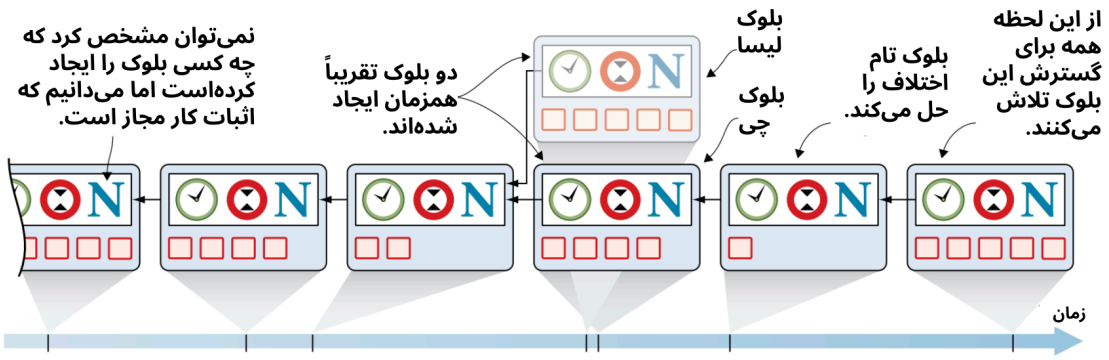
با اثبات کار، برای تعیین معتبر بودن یک بلوک به چیزی جز خود بلاک‌چین نیاز ندارید. پیش‌تر به اطلاعاتی خارج از بلاک‌چین، یعنی کلید عمومی[۲۸] استخراجگر از تابلوی اعلانات، نیاز داشتید. این جهشی بزرگ به سوی غیرمتمرکزسازی است؛ زیرا دیگر هیچ منبع مرکزی قابل‌دست‌کاری برای کلیدهای عمومی باقی نمانده است.

۳.۲.۷ مقایسه با اعداد خوش‌شانس

بلاک‌چین مانند قبل رشد می‌کند، با این تفاوت که انتخاب اعداد خوش‌شانس باچکیده گرفتن از سرآیند بلوک جایگزین شده است (شکل ۲۰.۷). جدول ۱.۷ این دو سامانه را مقایسه می‌کند.

به‌جای انتخاب یک عدد تصادفی در هر ثانیه، استخراجگرها از طریقچکیده‌سازی رمزنگاری، تقریباً هر ۰۲.۰ میکروثانیه یک عدد انتخاب می‌کنند. در عین حال، حد عدد

[۲۸] Public key – معادل فارسی: کلید عمومی



شکل ۲۰.۷: بلاک‌چین همانند زمانی عمل می‌کند که از اعداد خوش‌شانس استفاده می‌شد.

خوش‌شانس یا همان هدف، به‌جای ۵۵۵، روی عدد ۲۵۶بیتی e...۰۰۰۰۰۰۰۰۰۹۲۶ = ۹eb۹۲۶ × ۲^۲۰۰ قرار می‌گیرد.

مقایسهٔ روش اعداد خوش‌شانس و اثبات کار.

مفهوم	مقادیر هدف	هر چند وقت یک‌بار آزمون انجام می‌شود	میانگین زمان بلوک	زنجیرهٔ برتر در انشعاب
اعداد خوش‌شانس	۵۵۵	۱۰۰۰۰۰۰	هر ثانیه	۱۰ دقیقه
اثبات کار	۹eb۹۲۶ × ۲^۲۰۰	۲^۲۵۶	هر ۰۲.۰ میکروثانیه	۱۰ دقیقه

عدد ۰۲.۰ میکروثانیه فقط نمونه‌ای از مدت‌زمان یک «تلاش» است و این زمان از یک استخراجگر به استخراجگر دیگر تفاوت دارد.

تفاوتی ظریف اما مهم این است که در اثبات کار، شاخه‌ای بهترین شاخه برای پیروی محسوب می‌شود که بیشترین اثبات کار انباشته را داشته باشد. در روش اعداد خوش‌شانس، گره‌ها از طولانی‌ترین زنجیره پیروی می‌کردند. اثبات کار انباشتهٔ یک بلاک‌چین، مجموع سختی[۲۹] تمام بلوک‌های منفرد آن زنجیره است.

سختی یک بلوک معیاری است از اینکه یافتن اثبات کار معتبر برای آن بلوک، نسبت به یافتن آن برای بلوک پیدایش[۳۰]، چند برابر دشوارتر است.

به‌طور دقیق‌تر، سختی بلوک B این‌گونه محاسبه می‌شود: هدف بلوک پیدایش بر هدف بلوک B تقسیم می‌شود. در نتیجه، سختی بلوک پیدایش دقیقاً برابر با ۱ است.

مفهوم اصلی این است که هرچه هدف یک بلوک بزرگ‌تر باشد، سختی آن بلوک کمتر است و هرچه هدف کوچک‌تر باشد، سختی بیشتر است. بنابراین برای محاسبهٔ اثبات

[۲۹] Difficulty – معادل فارسی: سختی
[۳۰] Genesis block – معادل فارسی: بلوک پیدایش

کار انباشتهٔ یک زنجیره، سختی همهٔ بلوک‌های زنجیره را با یکدیگر جمع می‌کنیم.

زنجیرهٔ قدرتمندتر

از این پس، شاخه‌ای را که بیشترین کار انباشته را دارد «شاخهٔ قدرتمندتر» یا «زنجیرهٔ قدرتمندتر» می‌نامم. اصطلاح رایج دیگر، «بهترین زنجیره» است. تمایز میان طولانی‌ترین و قدرتمندترین زنجیره، هنگامی که تنظیم سختی را معرفی کنم، در بخش «قدرت زنجیره در برابر طول زنجیره» اهمیت پیدا می‌کند.

زنجیرهٔ قدرتمندتر زنجیرهٔ قدرتمندتر، زنجیره‌ای است که بیشترین اثبات کار انباشته را دارد.

۴.۲.۷ اگر نانس‌ها تمام شوند چه؟

تک‌بار یک عدد ۳۲بیتی است که مقدار کوچکی محسوب می‌شود. اگر یک استخراجگر همهٔ ۲۹۶,۹۶۷,۲۹۴,۴ مقدار ممکن را بدون موفقیت امتحان کند، باید برای تغییر سرآیند بلوک کار دیگری انجام دهد؛ وگرنه دقیقاً همان تلاش‌های قبلی را تکرار خواهد کرد. چند راه برای ایجاد تغییر وجود دارد (شکل ۲۱.۷):

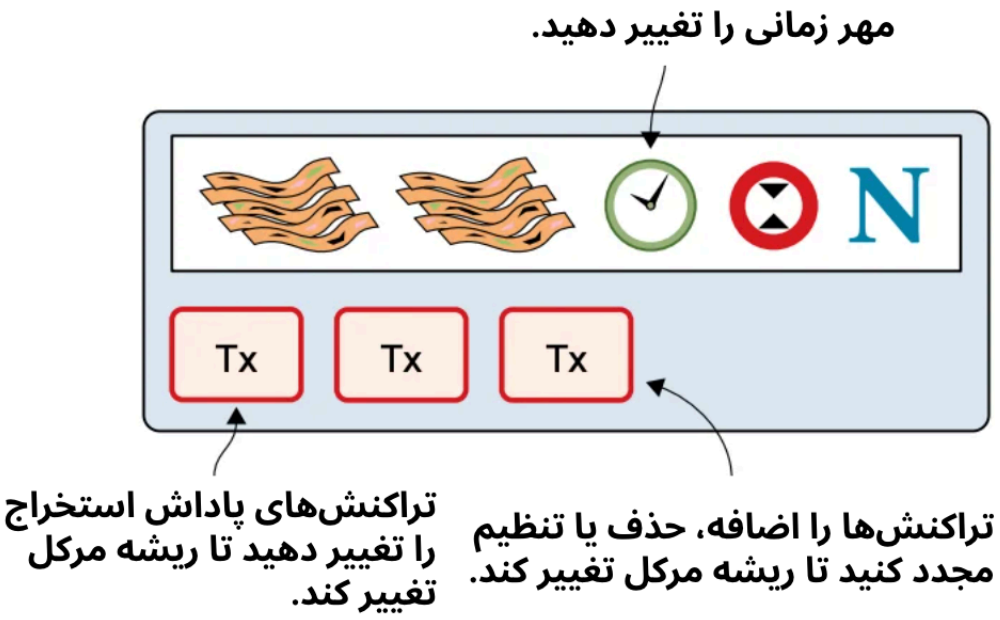
مهر زمانی را اندکی تغییر دهد.

تراکنش‌هایی را اضافه، حذف یا جابه‌جا کند.

تراکنش پاداش استخراج را تغییر دهد.

تغییر مهر زمانی ساده است؛ کافی است یک ثانیه به آن اضافه کنید تا سرآیند متفاوت شود. اگر از یکی از دو روش دیگر استفاده کنید، چون دادهٔ تراکنش تغییر کرده است، باید ریشهٔ مرکل را دوباره محاسبه کنید. با به‌روزرسانی ریشهٔ مرکل، سرآیند نیز تغییر می‌کند.

پس از هرکدام از این تغییرها در بلوک، سرآیند تغییر می‌کند؛ بنابراین تک‌بار را می‌توان دوباره روی صفر گذاشت و استخراجگر می‌تواند چکیده‌سازی را از نو آغاز کند.



شکل ۲۱.۷: سرآیند بلوک را می‌توان به روش‌های گوناگون تغییر داد.

۳.۷ ماینرها باید نقل مکان کنند

شرکت، سامانهٔ اثبات کار را خوب می‌داند، اما نمی‌خواهد هزینهٔ برق لازم برای انجام این همه کار را بپردازد. از آنجا که رایانه‌ها با برق کار می‌کنند، هرچه یک رایانه محاسبات بیشتری انجام دهد، برق بیشتری نیاز دارد.

شرکت تصمیم می‌گیرد استخراجگرها باید نرم‌افزار استخراج خود را در جای دیگری، مانند خانه‌هایشان، اجرا کنند. این تصمیم منصفانه است. به‌هرحال، استخراجگرها برای هر بلوکی که پیدا می‌کنند ۵۰ CT پاداش می‌گیرند و هزینهٔ برق تولید یک بلوک برای آن‌ها کمتر از ۵۰ CT است.

ارزش بازار فعلی ۵۰ CT برابر با پنج کلوچه در کافه است و هر توکن کلوچه در حال حاضر حدود ۲۰ سنت معامله می‌شود. هر بلوک تقریباً ۱۰ دلار توکن کلوچه به یک استخراجگر می‌رساند که با توجه به اینکه هر استخراجگر حدود ۴۸ بلوک در روز تولید می‌کند، مقدار قابل‌قبولی است.

بیایید نرخ چکیده‌سازی[۳۱] سه استخراجگر خود را به‌سرعت بررسی کنیم. نرخ

[۳۱] Hashrate – معادل فارسی: نرخ چکیده‌سازی

چکیده‌سازی معیاری است از تعداد چکیده‌ها، یا تلاش‌ها، که آن‌ها می‌توانند در هر ثانیه انجام دهند:

نرخ چکیده‌سازی و تعداد بلوک مورد انتظار استخراجگرها پیش از افزایش نرخ چکیده‌سازی.

استخراجگر	نرخ چکیده‌سازی، میلیون چکیده در ثانیه	بلوک موردانتظار در روز
لیسا	۱۰۰	۴۸
تام	۱۰۰	۴۸
چی	۱۰۰	۴۸
مجموع	۳۰۰	۱۴۴

این سامانه تقریباً ۱۴۴ بلوک در روز تولید می‌کند؛ یعنی به‌طور میانگین یک بلوک در هر ۱۰ دقیقه.

۱.۳.۷ افزودن نرخ هش بیشتر

ویژگی جالب این سامانه آن است که هرکس می‌تواند بدون گرفتن اجازه استخراجگر شود. کافی است در خانهٔ خود یک رایانه راه‌اندازی کند و ساختن بلوک را آغاز کند. دیگر بلوک‌ها به یک شخص وابسته نیستند، بلکه به مقدار کار محاسباتی وابسته‌اند:

لیسا نرخ چکیده‌سازی خود را افزایش می‌دهد: لیسا استخراج در خانه را کسب‌وکاری سودآور می‌داند. او تصمیم می‌گیرد یک رایانهٔ مشابه دیگر به خانه‌اش اضافه کند که عملاً نرخ چکیده‌سازی او را دو برابر می‌کند.

رشید استخراجگر می‌شود: رشید نیز می‌خواهد وارد کسب‌وکار استخراج شود. او در خانه رایانه‌ای راه‌اندازی می‌کند که برای بلوک‌های جدید رقابت می‌کند. رایانهٔ او کمی سریع‌تر از رایانهٔ رقباست؛ بنابراین انتظار دارد، برای مثال، از چی بلوک‌های بیشتری در روز تولید کند.

پس از افزایش نرخ چکیده‌سازی توسط لیسا و رشید، نرخ چکیده‌سازی کل سامانهٔ توکن کلوچه به‌طور چشمگیری افزایش می‌یابد:

نرخ چکیده‌سازی و تعداد بلوک مورد انتظار پس از ورود استخراجگرهای جدید.

استخراجگر	نرخ چکیده‌سازی، میلیون چکیده در ثانیه	بلوک موردانتظار در روز
لیسا	۲۰۰	۹۶
تام	۱۰۰	۴۸
چی	۱۰۰	۴۸
رشید	۱۵۰	۷۲
مجموع	۵۵۰	۲۶۴

نرخ چکیده‌سازی کل بیت‌کوین

در زمان نگارش کتاب، نرخ چکیده‌سازی کل بیت‌کوین حدود ۵۰ اگزاهش در ثانیه است؛ یعنی ۵۰×۱۰^{۱۸} چکیده در ثانیه.

ببینید: اکنون در روز بیش از مقداری که طراحی کرده بودیم بلوک تولید می‌کنیم. هدف، ۱۴۴ بلوک در روز است؛ اما ۲۶۴ به‌طور قابل‌توجهی بیشتر است. نرخ تولید بلوک بیش از حد بالاست و تقریباً دو برابر نرخ مطلوب شده است.

۲.۳.۷ مشکلات نرخ بالای تولید بلوک

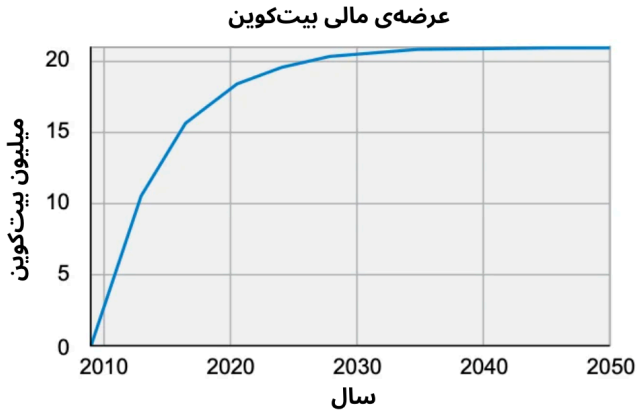
ممکن است نرخ بالاتر تولید بلوک سودمند به نظر برسد، زیرا زمان تأیید تراکنش‌ها را کاهش می‌دهد؛ اما مشکلاتی نیز به همراه دارد.

ایجاد بیش از حد سریع پول

منحنی عرضهٔ پول برنامه‌ریزی‌شده از فصل ۲ را به یاد بیاورید. برنامه این بود که نیمی از عرضهٔ پول، یعنی ۵.۱۰ میلیون CT، در چهار سال نخست منتشر شود؛ سپس طی چهار سال بعد، نیمی از آن مقدار، یعنی ۲۵.۵ میلیون CT، منتشر شود؛ و این روند ادامه یابد تا میزان انتشار به صفر گرد شود. کل این فرایند حدود ۱۳۱ سال طول می‌کشد.

اما اکنون، چون لیسا توان استخراج خود را افزایش داده و رشید رایانهٔ استخراج خود

را افزوده است، انتشار پول بیش از حد سریع شده است. با این نرخ بالای تولید بلوک، زمان لازم برای ایجاد همهٔ توکن‌های کلوچه فقط نصف خواهد شد.



یعنی نرخ افزایش عرضهٔ پول برابر با $\frac{۲۶۴}{۱۴۴} = ۱/۸$ برابر نرخ افزایش عرضهٔ مطلوب است.

انشعاب‌های بیشتر

انشعاب‌ها هر از گاهی به‌طور طبیعی رخ می‌دهند؛ اما با افزایش نرخ تولید بلوک، خطر انشعاب‌های طبیعی نیز بیشتر می‌شود. تصور کنید ۰۰۰٫۳ نفر در زیرزمین خانه‌هایشان شروع به استخراج کنند. در این صورت، نرخ تولید بلوک هزار برابر افزایش می‌یابد. در هر ثانیه، چندین استخراجگر اثبات کار معتبری پیدا می‌کنند و بلوکی منتشر می‌کنند. تقریباً در هر ارتفاع بلوک، انشعاب رخ می‌دهد.

این وضعیت، تراکنش‌های موجود در بلوک‌های اخیر را کم‌اعتمادتر می‌کند؛ زیرا این بلوک‌ها آسان‌تر می‌توانند از زنجیرهٔ اصلی جدا شوند. همچنین از منظر امنیتی مشکل‌ساز است؛ زیرا اگر دو شاخه هرکدام حدود ۵۰ درصد از کل نرخ چکیده‌سازی را در اختیار داشته باشند، امنیت هر شاخه به نصف کاهش می‌یابد. در بخش «استخراجگرها چه آسیب‌هایی می‌توانند وارد کنند؟» امنیت بلاک‌چین را بیشتر بررسی خواهیم کرد.

۳.۳.۷ چه چیزی برطرف شده است؟

ما مسئلهٔ دشوار وادارکردن استخراجگرها به انتخاب «اعداد خوش‌شانس صادقانه» را به شیوه‌ای جالب حل کرده‌ایم. حالا ببینیم چه مشکلاتی از بخش «احتمال انشعاب‌ها»

باقی مانده‌اند.

می‌توان با اعداد خوش‌شانس تقلب کرد. نمی‌توان ثابت کرد که واقعاً یک عدد خوش‌شانس را صادقانه انتخاب کرده‌اید.

با هر استخراجگر جدید، سامانه در برابر سانسور مقاوم‌تر، اما در برابر سرقت کلید خصوصی آسیب‌پذیرتر می‌شود. کلید خصوصی سرقت‌شده برای امضای بلوک، به سارق اجازه می‌دهد با تقلب در انتخاب اعداد خوش‌شانس بلوک بسازد و پاداش‌ها را برای خود بردارد.

با افزوده‌شدن هر استخراجگر، خطر تقلب‌کردن یکی از استخراجگرها در انتخاب اعداد خوش‌شانس افزایش می‌یابد.

نمی‌توان صرفاً استخراجگرهای جدیدی به سامانه افزود. با افزایش تعداد استخراجگرها، باید آستانهٔ عدد خوش‌شانس را پایین آورد تا میانگین ۱۰ دقیقه برای هر بلوک و نرخ انتشار پول در سطح مطلوب حفظ شود.

فقط یک مسئله از این فهرست باقی مانده است که در بخش بعدی حل می‌کنیم.

۴.۷ تنظیم سختی

اکنون که استخراجگرها و نرخ چکیده‌سازی بیشتری به سامانه افزوده‌اید، نرخ تولید بلوک افزایش یافته است. علت این است که استخراجگرها در مجموع نسبت به قبل، در هر ثانیه تلاش‌های بیشتری انجام می‌دهند و در نتیجه در هر ساعت بلوک‌های بیشتری تولید می‌شود.

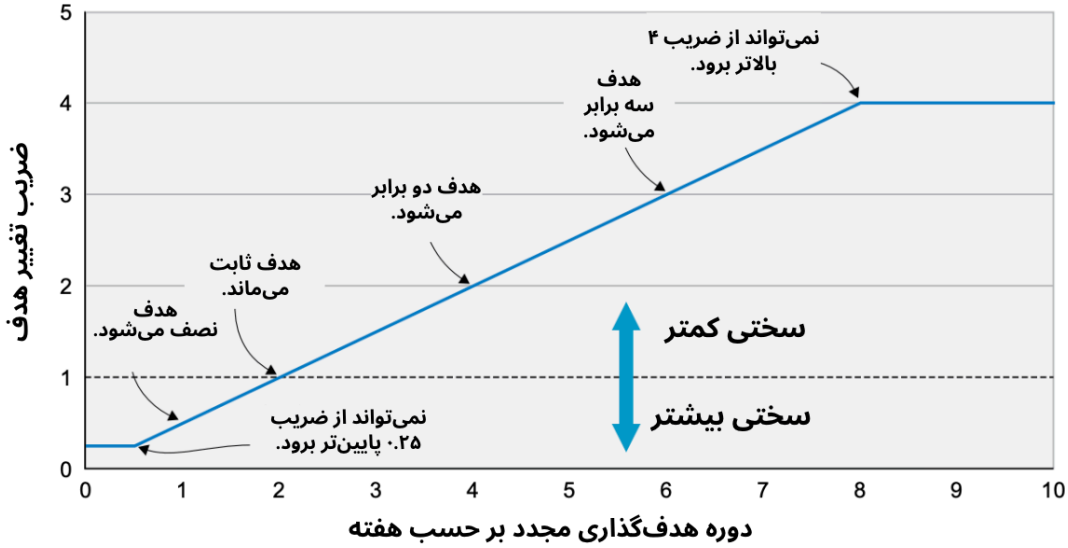
همه بر سر هدف موجود در سرآیند بلوک توافق کرده‌اند، اما برای سازگاری با افزایش یا کاهش نرخ چکیده‌سازی کل، باید سختی استخراج یک بلوک را تنظیم کنید. هدف پس از هر ۰۱۶٫۲ بلوک تنظیم می‌شود. این تنظیم، «تنظیم سختی» یا «تنظیم مجدد هدف» نام دارد و دورهٔ ۰۱۶٫۲ بلوکی را «دورهٔ تنظیم مجدد» می‌نامند.

به یاد داشته باشید که هر بلوک یک تراکنش پاداش استخراج دارد که ۵۰ توکن کلوچه جدید ایجاد می‌کند. برای حفظ نرخ مطلوب انتشار توکن‌های کلوچه جدید، می‌خواهید به‌طور میانگین هر ۱۰ دقیقه یک بلوک تولید شود. تولید ۰۱۶٫۲ بلوک با

این نرخ، دو هفته زمان می‌برد.

اگر دورهٔ تنظیم مجدد قبلی بیش از دو هفته طول کشیده باشد، هدف باید افزایش یابد تا احتمال رسیدنچکیده سرآیند بلوک به آن بیشتر شود؛ یعنی سختی کاهش می‌یابد. اگر این دوره کمتر از دو هفته طول کشیده باشد، باید هدف را کاهش دهید تا احتمال رسیدن به آن کمتر شود؛ یعنی سختی افزایش می‌یابد.

هدف جدید، N، از رابطهٔ $F \times O = N$ محاسبه می‌شود؛ در این رابطه O هدف قدیمی و F ضریب تغییر هدف است که به طول دورهٔ تنظیم مجدد گذشته بستگی دارد؛ همان‌گونه که شکل ۲۲.۷ نشان می‌دهد.



شکل ۲۲.۷: تنظیم هدف بر اساس ۰۱۶٫۲ بلوک گذشته؛ هدف، تولید ۰۱۶٫۲ بلوک در دو هفته است.

به‌طور کلی، هدف جدید N از هدف قدیمی O و مدت‌زمان T دورهٔ تنظیم مجدد گذشته محاسبه می‌شود:

$$N = O * \begin{cases} \frac{1}{4} & \text{if } T < 0.5 \\ \frac{T}{2} & \text{if } 0.5 \leq T \leq 8 \\ 4 & \text{if } 8 < T \end{cases}$$

هدف نمی‌تواند بیش از چهار برابر افزایش یا کمتر از یک‌چهارم کاهش یابد. این

محدودیت، اثر بعضی حملات خرج مضاعف[۳۲] را کاهش می‌دهد؛ حملاتی که در آن مهاجم، گره قربانی را از گره‌های درست‌کار جدا می‌کند تا سختی را به نفع خود دست‌کاری کند.

۱.۴.۷ قواعد مهر زمانی

سرآیند بلوک شامل مهر زمانی است. مهرهای زمانی اهمیت دارند، زیرا می‌خواهید سامانه بدون دخالت انسان و به‌طور خودکار هدف را تنظیم کند تا به‌طور میانگین هر ۱۰ دقیقه یک بلوک ایجاد شود. نرخ ایجاد بلوک مهم است، زیرا می‌خواهید انتشار توکن‌های کلوچه جدید قابل‌پیش‌بینی باشد.

مهرهای زمانی

مهرهای زمانی در برخی امکانات و ویژگی‌های تراکنش‌ها نیز به کار می‌روند که در فصل ۹ بیشتر دربارهٔ آن‌ها صحبت خواهد شد.

استخراجگری که یک بلوک ایجاد می‌کند، پیش از تولید اثبات کار، مهر زمانی را روی زمان فعلی قرار می‌دهد. اما چون گره‌های کامل گوناگون روی رایانه‌های متفاوت اجرا می‌شوند، ممکن است ساعت آن‌ها کاملاً همگام نباشد.

فرض کنید لیسا بلوکی با مهر زمانی ۲۰۱۷-۰۸-۱۳ ۲۱:۳۳:۰۷ UTC ایجاد می‌کند و آن را در پوشهٔ اشتراکی قرار می‌دهد. سپس تام بلوک بعدی را تولید می‌کند، اما ساعت او از ساعت لیسا عقب‌تر است.

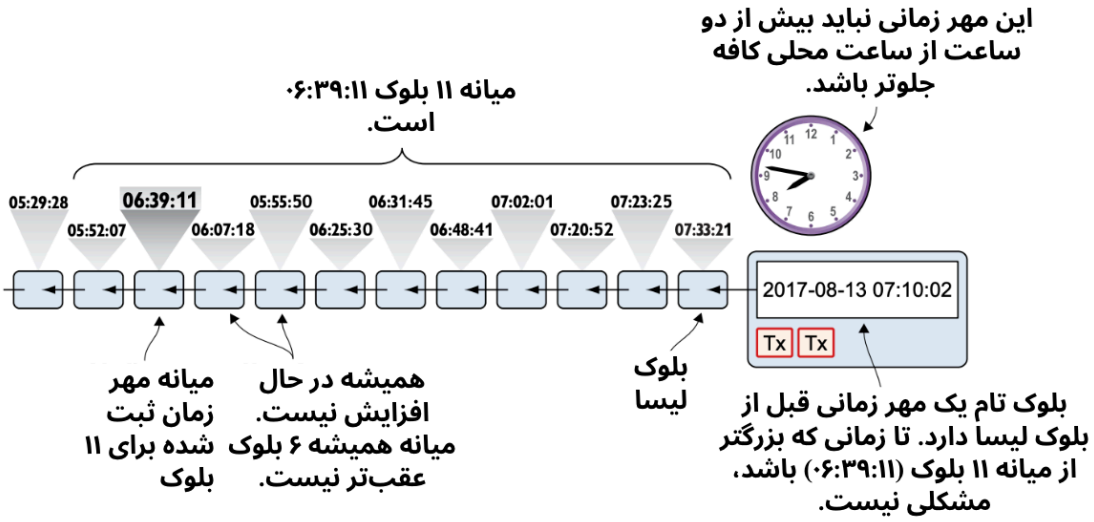
تام بلوکی با مهر زمانی زودتر از مهر زمانی بلوک قبلی ایجاد می‌کند. این موضوع تا زمانی که مهرهای زمانی اختلاف زیادی نداشته باشند، مشکل‌ساز نیست (شکل ۲۳.۷).

مهر زمانی باید از چند قاعده پیروی کند. فرض کنید گرهٔ کامل کافه در آستانهٔ اعتبارسنجی بلوک تام است:

مهر زمانی باید حتماً از میانهٔ ۱۱ مهر زمانی پیشین جدیدتر باشد. این میانه معمولاً «میانهٔ زمان گذشتهٔ بلوک[۳۳]» نامیده می‌شود.

مهر زمانی، بر اساس ساعت کافه، حداکثر می‌تواند دو ساعت در آینده باشد.

[۳۲] Double spending – معادل فارسی: خرج مضاعف
[۳۳] Median Time Past – معادل فارسی: میانهٔ زمان گذشته



شکل ۲۳.۷: دو بلوک با مهرهای زمانی کاهشی استخراج می‌شوند؛ این موضوع اشکالی ندارد.

این قواعد تضمین می‌کنند که کسی نتواند مهر زمانی بلوک‌های خود را برای اثرگذاری بر محاسبهٔ هدف بعدی دست‌کاری کند. تصور کنید آخرین بلوک پیش از تنظیم مجدد، مهر زمانی شش هفته پس از زمان فعلی داشته باشد. در این حالت، هدف بعدی چهار برابر افزایش می‌یابد؛ همان‌طور که جدول ۲.۷ نشان می‌دهد.

جدول ۲.۷: نمونه‌ای از مهرهای زمانی در یک دورهٔ تنظیم سختی.

ارتفاع بلوک	مهر زمانی، بدون درنظرگرفتن ثانیه	زمان سپری‌شده بر اساس مهر زمانی
H	۳۱:۰۶ ۳۱-۰۷-۲۰۱۷	۰
۱ + H	۴۲:۰۶ ۳۱-۰۷-۲۰۱۷	۱۱ دقیقه و ۱۷ ثانیه
...	...	...
۰۱۳،۲ + H	۲۲:۰۷ ۱۴-۰۸-۲۰۱۷	۲ هفته و ۵۱ دقیقه
۰۱۴،۲ + H	۳۳:۰۷ ۱۴-۰۸-۲۰۱۷	۲ هفته و ۱ ساعت و ۲ دقیقه
۰۱۵،۲ + H	۵۱:۰۸ ۲۵-۰۹-۲۰۱۷	۸ هفته و ۲ ساعت و ۲۰ دقیقه

آخرین مهر زمانی، شش هفته دیرتر از زمانی است که بلوک واقعاً استخراج شده است. تمام گره‌های کامل این بلوک را رد می‌کنند، زیرا قواعد مهر زمانی را نقض می‌کند. مشخص است که فردی در تلاش است هدف را دست‌کاری کند.

اگر این بلوک پذیرفته می‌شد، هدف بعدی چهار برابر هدف فعلی می‌شد؛ در نتیجه

یافتن اثبات کار معتبر چهار برابر آسان‌تر می‌شد. قواعد مهر زمانی توضیح‌داده‌شده، این نوع رفتار نادرست را ممنوع می‌کنند. از آنجا که نمی‌توانید بیش از دو ساعت در مهر زمانی خود دروغ بگویید، هدف بعدی نیز فقط در حد بسیار اندکی قابل دست‌کاری است.

۲.۴.۷ قدرت زنجیره در برابر طول زنجیره

به بحث قدرت زنجیره و اهمیت توجه‌نکردن صرف به طول زنجیره برگردیم. از نظر شهودی، هرچه بازنویسی تاریخچهٔ زنجیره دشوارتر باشد، بهتر است؛ بنابراین باید از قدرتمندترین زنجیره پیروی کنید. اما چه زمانی قدرتمندترین و طولانی‌ترین زنجیره با هم تفاوت دارند؟

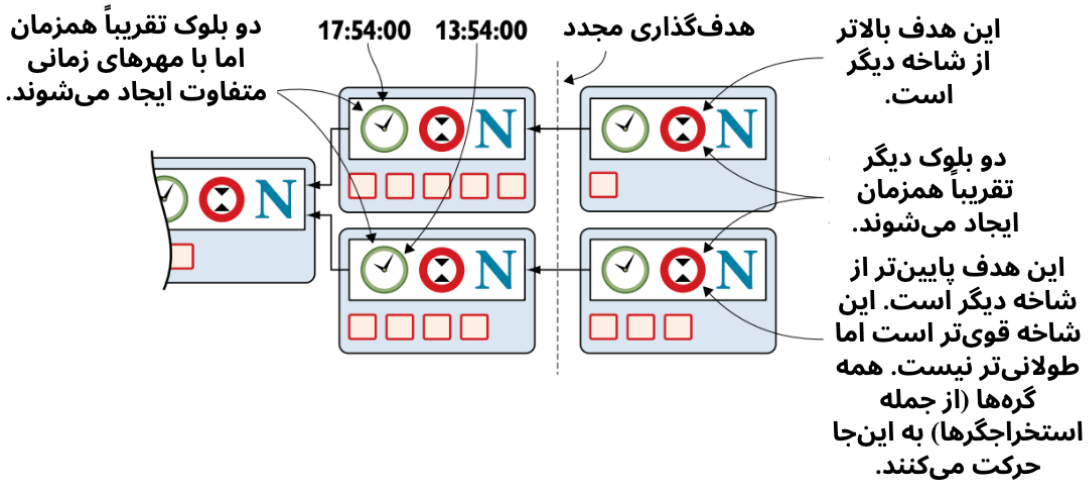
این تفاوت می‌تواند به دلایل زیر ایجاد شود:

انشعاب طبیعی درست پیش از تنظیم مجدد؛

انشعاب‌های تصادفی ناشی از نسخه‌های ناسازگار نرم‌افزار؛

انشعاب‌های عمدی، به‌عنوان حمله علیه زنجیرهٔ درست‌کار.

در اینجا فقط حالت نخست را بررسی می‌کنیم. فرض کنید یک انشعاب طبیعی رخ دهد (شکل ۲۴.۷).



شکل ۲۴.۷: انشعاب طبیعی با مهرهای زمانی متفاوت در دو شاخه، در صورت وقوع تنظیم مجدد باعث می‌شود یکی از شاخه‌ها از دیگری قدرتمندتر شود.

این سناریو بعید است، اما باید آن را در نظر گرفت، زیرا ممکن است رخ دهد. درست پیش از یک تنظیم مجدد، انشعابی رخ می‌دهد و مهر زمانی دو بلوک چهار ساعت با هم تفاوت دارد. سپس دو بلوک جدید به‌طور هم‌زمان تولید می‌شوند؛ یکی روی هر شاخه. این بلوک‌های جدید بر مبنای تاریخچه‌های متفاوت، تنظیم مجدد شده‌اند.

آخرین مهر زمانی در دوره‌های تنظیم مجدد دو شاخه، چهار ساعت با یکدیگر تفاوت دارد و در نتیجه اهداف جدید نیز متفاوت می‌شوند. فرمول تنظیم مجدد هدف را به یاد بیاورید.

از آنجا که اهداف جدید متفاوت‌اند، سختی جدید آخرین بلوک در هر شاخه نیز متفاوت است. یعنی قدرت زنجیره تفاوت پیدا می‌کند، زیرا شاخه‌ها اکنون اثبات کار انباشتهٔ متفاوتی دارند.

۵.۷ ماینرها چه آسیب‌هایی می‌توانند وارد کنند؟

در فصل ۶ مطمئن شدید که لیسا نمی‌تواند تراکنش‌ها را بدون آشکارکردن تلاش خود برای تقلب، لغو کند. این کار را با ملزم‌کردن لیسا به امضای دیجیتال بلوک‌ها انجام دادید تا هرکس بتواند تأیید کند لیسا یک بلوک را تأیید کرده است. اگر او بعداً در همان ارتفاع، بلوک متعارضی را امضا کند که تراکنش خودش را با تراکنشی که به خودش پرداخت می‌کند جایگزین کند، همه متوجه می‌شوند و می‌توانند او را پاسخ‌گو بدانند.

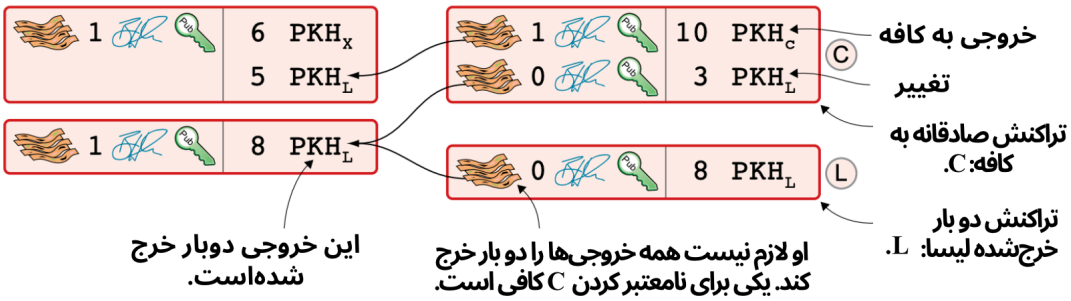
اکنون وضعیت متفاوت است. لیسا دیگر بلوک‌هایش را امضا نمی‌کند. بلوک‌ها ناشناس‌اند و چیزی لیسا را به یک بلوک مشخص پیوند نمی‌دهد. آیا این بدان معناست که او دوباره می‌تواند خرج مضاعف انجام دهد؟

بله؛ اگر بسیار خوش‌شانس باشد.

۱.۵.۷ خرج مضاعف

فرض کنید لیسا می‌خواهد برای خرید یک کلوچه در کافه پرداخت کند. اما هم‌زمان با پرداخت، تراکنش خرج مضاعف را نیز آماده می‌کند (شکل ۲۵.۷).

C تراکنش پرداخت به کافه است و L تراکنش خرج مضاعف لیساست که می‌خواهد با



شکل ۲۵.۷: لیسا دو تراکنش ایجاد می‌کند که هر دو یک خروجی مشترک را خرج می‌کنند.

آن پولش را پس بگیرد. هر دو تراکنش به‌تنهایی کاملاً معتبرند، اما نمی‌توانند هم‌زمان هر دو معتبر باشند، زیرا هر دو یک خروجی مشترک را خرج می‌کنند. هر خروجی فقط یک بار قابل خرج‌کردن است.

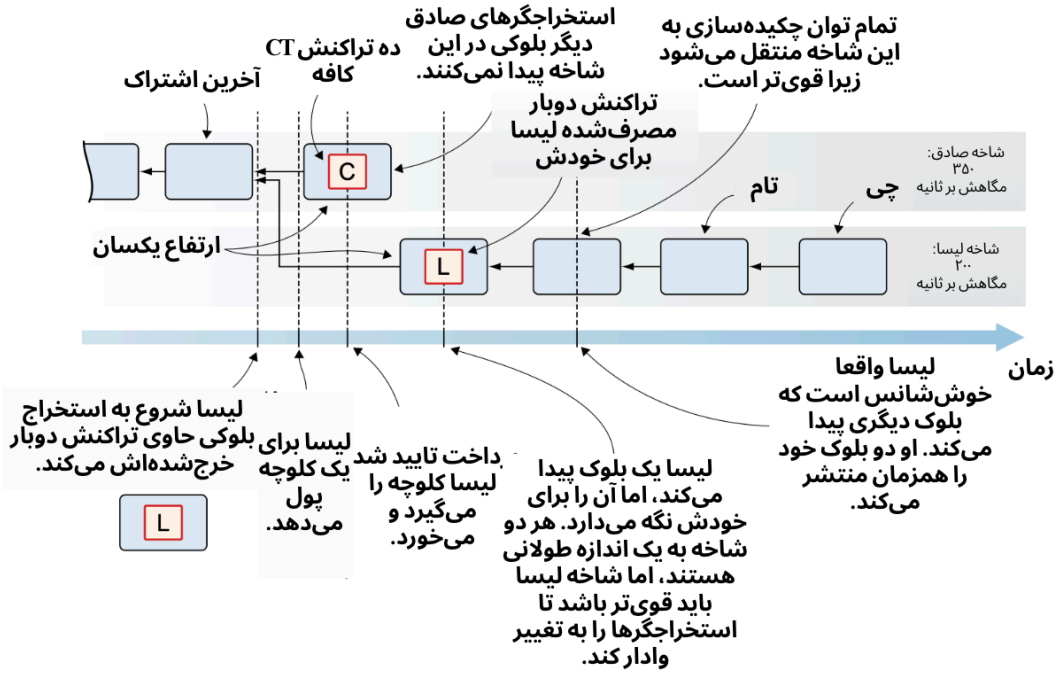
لیسا پرداخت درست‌کارانه، یعنی C، را برای همهٔ استخراجگرها می‌فرستد. در حالی که استخراجگرهای دیگر می‌کوشند تراکنش درست‌کارانهٔ او را وارد بلوکی کنند و برای آن اثبات کار معتبر بیابند، لیسا به‌طور مخفی تراکنش خرج مضاعف، یعنی L، را در بلوک مخفی خود قرار می‌دهد و کار روی آن بلوک را آغاز می‌کند (شکل ۲۶.۷).

هدف لیسا این است که به‌طور مخفی برای شاخهٔ متقلبانهٔ حاوی L، اثبات کار معتبری بیابد که از اثبات کار زنجیرهٔ درست‌کار بیشتر باشد. اگر موفق شود، همهٔ بلوک‌های شاخهٔ خود را منتشر می‌کند؛ همهٔ استخراجگرها به شاخهٔ او منتقل می‌شوند و به‌جای شاخهٔ پیشین، شاخهٔ او را ادامه می‌دهند.

برای سادگی، فرض کنید هیچ تنظیم مجددی رخ نمی‌دهد و در میانهٔ یک دورهٔ تنظیم مجدد هستیم. در نتیجه، همهٔ بلوک‌ها هدف، یا سختی، یکسانی دارند و می‌توانیم به‌جای قدرت شاخه، صرفاً طول شاخه را بررسی کنیم.

گروهی از استخراجگرها در تلاش‌اند تراکنش درست‌کارانهٔ لیسا، C، را تأیید کنند؛ در حالی که لیسا می‌کوشد برای بلوک حاوی تراکنش خرج مضاعف، L، اثبات کار معتبر بیابد. کافه پیش از تحویل کلوچه، منتظر تراکنش معتبر می‌ماند.

سرانجام تراکنش درست‌کارانه در زنجیرهٔ درست‌کار تأیید می‌شود. کافه آن بلوک را می‌بیند، اعتبارش را بررسی می‌کند و کلوچه را به لیسا می‌دهد. لیسا آن را می‌خورد. هنگامی که آخرین خردهٔ کلوچه را قورت می‌دهد، رایانه‌اش به‌طور اتفاقی برای بلوک خود اثبات کار معتبر پیدا می‌کند.



شکل ۲۶.۷: لیسا حملهٔ خرج مضاعف انجام می‌دهد و با وجود نرخ چکیده‌سازی پایین‌تر خود، موفق می‌شود.

او هنوز بلوکش را منتشر نمی‌کند، زیرا در این مرحله سودی ندارد. استخراجگرها از پیش روی شاخهٔ درست‌کار استخراج می‌کنند، زیرا نخستین بلوکی بوده است که دیده‌اند.

نرخ چکیده‌سازی ترکیبی همهٔ استخراجگرها روی زنجیرهٔ درست‌کار، ۳۵۰ مگاهش بر ثانیه است؛ در حالی که لیسا فقط ۲۰۰ مگاهش بر ثانیه دارد. بنابراین، انتظار می‌رود زنجیرهٔ درست‌کار بیش از لیسا بلوک پیدا کند.

اما همه گاهی خوش‌شانس می‌شوند. لیسا خوش‌شانس است و بلوک دیگری نیز روی شاخهٔ متقلبانهٔ خود پیدا می‌کند. اکنون شاخهٔ او دو بلوک دارد، اما زنجیرهٔ درست‌کار فقط یک بلوک دارد. شاخهٔ لیسا اثبات کار بیشتری از شاخهٔ استخراجگرهای درست‌کار دارد؛ بنابراین او دو بلوک خود را در پوشهٔ اشتراکی منتشر می‌کند.

از کدام شاخه باید پیروی کرد؟

لازم نیست یک استخراجگر همیشه روی نخستین بلوکی که می‌بیند استخراج کند؛ اما بیت‌کوین کور، یعنی رایج‌ترین نرم‌افزار بیت‌کوین، از نخستین بلوک مشاهده‌شده پیروی می‌کند.

استخراجگرهای دیگر این دو بلوک را می‌بینند، متوجه می‌شوند شاخهٔ لیسا اثبات کار بیشتری از شاخهٔ درست‌کار دارد و به شاخهٔ لیسا منتقل می‌شوند. استخراجگرهایی که منتقل می‌شوند نمی‌توانند تشخیص دهند جرمی رخ داده یا چه کسی بلوک‌ها را ایجاد کرده است؛ آن‌ها بی‌طرفانه به قدرتمندترین زنجیرهٔ معتبر می‌پیوندند.

در نتیجه، تراکنش C برای کافه عملاً لغو می‌شود. این تراکنش دیگر بخشی از زنجیره‌ای با بیشترین اثبات کار نیست. کافه ۱۰ CT را که هنگام تحویل کلوچه به لیسا تصور می‌کرد دریافت کرده است، از دست می‌دهد.

از این نقطه به بعد، بلوک‌های جدید شاخهٔ لیسا را گسترش می‌دهند و همه‌چیز به شکل عادی ادامه می‌یابد. بلوک حاوی تراکنش C از زنجیرهٔ اصلی کنار گذاشته می‌شود.

۲.۵.۷ محافظت در برابر حملات خرج مضاعف

با وجود اینکه احتمال موفقیت لیسا کم است، ممکن است خوش‌شانس شود و مانند مثال پیشین، در حملهٔ خرج مضاعف موفق شود. تلاش برای خرج مضاعف ۱۰ CT از نظر اقتصادی برای لیسا به‌صرفه نیست؛ زیرا اگر موفق نشود، خطر مصرف مقدار زیادی برق و از رده خارج‌شدن بلوک‌های خود را پذیرفته است و پاداش آن بلوک‌ها را از دست می‌دهد.

اما اگر بخواهد مقدار بزرگ‌تری، مثلاً ۱۰۰,۰۰۰ CT، را خرج مضاعف کند چه؟ در این صورت شاید این کار ارزش امتحان‌کردن داشته باشد. تصور کنید بتواند کل کافه را بخرد و سپس حملهٔ خرج مضاعف را انجام دهد. در آن صورت هم کافه را دارد و هم ۱۰۰,۰۰۰ CT خود را حفظ می‌کند.

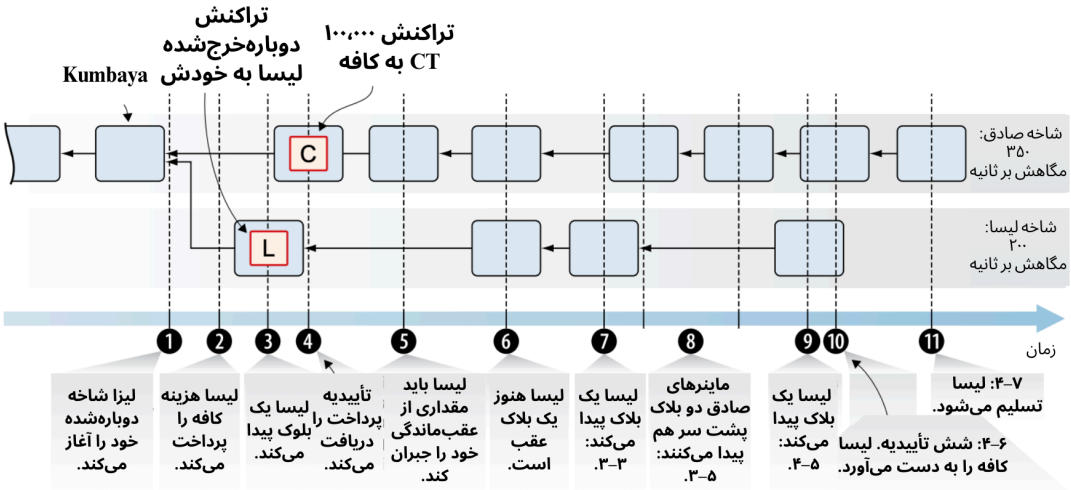
صاحب کافه حاضر است کافه را در برابر ۱۰۰,۰۰۰ CT به لیسا بفروشد؛ اما از حملات خرج مضاعف آگاه است. بنابراین به لیسا می‌گوید برای چنین مبلغی، کافه را پس از شش تأیید به او واگذار می‌کند.

این یعنی لیسا باید ۱۰۰,۰۰۰ CT به صاحب کافه بپردازد و سپس صبر کند تا تراکنش در یک بلوک قرار بگیرد و پس از آن، پنج بلوک دیگر ساخته شود. فقط پس از آن است که صاحب کافه، کافه را به لیسا تحویل می‌دهد.

برای موفق‌شدن در حملهٔ خرج مضاعف، لیسا باید هم‌زمان با انتظار کافه برای شش

تأیید، مانند حملهٔ قبلی یک شاخهٔ جایگزین را به‌طور مخفی بسازد. پس از آنکه صاحب کافه شش تأیید را دید و کافه را تحویل داد، لیسا باید در مقطعی شاخهٔ خرج مضاعف قدرتمندتری را در پوشهٔ اشتراکی منتشر کند. بنابراین، لیسا باید برای مدت طولانی‌تری نسبت به مثال پیشین خوش‌شانس بماند.

ببینیم این حمله چه نتیجه‌ای دارد (شکل ۲۷.۷).



شکل ۲۷.۷: لیسا می‌کوشد تراکنشی با شش تأیید را خرج مضاعف کند، اما شکست می‌خورد.

نتیجه همان‌طور است که انتظار می‌رود. لیسا در بلندمدت نتوانست بیش از زنجیرهٔ درست‌کار بلوک تولید کند و در امتیاز ۷ در برابر ۴ تسلیم شد.

جدول زیر دنبالهٔ رخدادهای این مثال را نشان می‌دهد:

لیسا به چند دلیل تسلیم می‌شود:

متوجه می‌شود نرخ چکیده‌سازی کافی برای جبران عقب‌ماندگی و پیشی‌گرفتن از زنجیرهٔ درست‌کار ندارد. در هر لحظه، احتمال اینکه لیسا بلوک بعدی را پیدا کند، ۲۰۰ / ۵۵۰ = ۳۶.۰ است. بنابراین احتمال اینکه استخراجگرهای درست‌کار بلوک بعدی را پیدا کنند، ۱ - ۳۶.۰ = ۶۴.۰ است. بلوک‌ها در زنجیرهٔ درست‌کار بسیار سریع‌تر پیدا خواهند شد.

در هر دقیقه‌ای که به تلاش ادامه می‌دهد، رایانهٔ او برق مصرف می‌کند و این برق هزینه دارد. اگر در تلاش خرج مضاعف موفق نشود، هزینهٔ برق بیهوده صرف شده است.

دنبالهٔ رخدادهای نمونهٔ حملهٔ خرج مضاعف.

رویداد	امتیاز C–L	توضیح
لیسا استخراج روی شاخهٔ مخفی حاوی تراکنش خرج مضاعف خود را آغاز می‌کند و پرداختی نیز برای استخراجگرهای درست‌کار می‌فرستد.	۰–۰	—
لیسا یک بلوک پیدا می‌کند، اما آن را مخفی نگه می‌دارد تا کافه متوجه حملهٔ خرج مضاعف نشود.	۰–۱	—
پرداخت درست‌کارانهٔ C نخستین تأیید خود را می‌گیرد. کافه پیش از انجام معامله، پنج بلوک دیگر صبر می‌کند.	۱–۱	—
لیسا به‌خوبی پیش می‌رود، اما یک بلوک عقب است و برای موفقیت باید دو بلوک بیشتر از کافه تولید کند.	۵–۴	—
تراکنش درست‌کارانه شش تأیید می‌گیرد. لیسا کافه را تحویل می‌گیرد و سند انتقال امضا می‌شود؛ با این حال، او همچنان برای جبران عقب‌ماندگی تلاش می‌کند.	۶–۴	—
لیسا می‌فهمد اوضاع ناامیدکننده است؛ احتمال اینکه در آینده چهار بلوک بیشتر از زنجیرهٔ درست‌کار بسازد بسیار اندک است.	۷–۴	—

برای هر بلوکی که روی زنجیرهٔ خودش استخراج می‌کند، در صورت شکست، پاداش ۵۰ CT آن بلوک را از دست خواهد داد.

نکتهٔ کلیدی این است که کافه شش تأیید درخواست کرده بود. هرچه تأییدهای موردنیاز بیشتر باشد، ساختن شاخه‌ای قدرتمندتر از شاخهٔ استخراجگرهای درست‌کار برای لیسا دشوارتر می‌شود. او به خوش‌شانسی بیشتری نیاز دارد.

وقتی کافه شش تأیید را دریافت کرد، لیسا دو بلوک عقب بود. او باید سریع‌تر از زنجیرهٔ درست‌کار رشد می‌کرد و یک بلوک از آن بلندتر می‌شد. شانس او اندک است. هرچه تعداد بلوک‌هایی که باید جبران کند بیشتر باشد، احتمال موفقیت نیز کمتر می‌شود؛ همان‌گونه که جدول ۳.۷ نشان می‌دهد.

تأییدها

با شش تأیید، تقریباً می‌توانید مطمئن باشید کسی علیه شما حملهٔ خرج مضاعف انجام نمی‌دهد. بااین‌حال، هرچه ارزش تراکنش بالاتر باشد، تلاش برای خرج مضاعف از نظر اقتصادی توجیه‌پذیرتر می‌شود.

جدول ۳.۷: احتمال جبران عقب‌ماندگی از دید مهاجم.

تعداد بلوک عقب‌ماندگی	نرخ چکیده‌سازی ۱٪	۱۰٪	۱۸٪، تام	۳۶٪، لیسا	۴۵٪	۵۰٪
۱	۰.۰۱۰۱۰۱	۰.۱۱۱۱۱۱	۰.۲۱۹۵۱۲	۰.۵۶۲۵۰۰	۰.۸۱۸۱۸۲	۰.۰۰۰۰۰۰۱
۲	۰.۰۰۰۱۰۲	۰.۰۱۲۳۴۶	۰.۰۴۸۱۸۶	۰.۳۱۶۴۰۶	۰.۶۶۹۴۲۱	۰.۰۰۰۰۰۰۱
۳	$۱/۰ \times ۱۰^{-۶}$	۰.۰۰۱۳۷۲	۰.۰۱۰۵۷۷	۰.۱۷۷۹۷۹	۰.۵۴۷۷۰۸	۰.۰۰۰۰۰۰۱
۴	$۱/۰ \times ۱۰^{-۸}$	۰.۰۰۰۱۵۲	۰.۰۰۲۳۲۲	۰.۱۰۰۱۱۳	۰.۴۴۸۱۲۵	۰.۰۰۰۰۰۰۱
۵	$۱/۱ \times ۱۰^{-۱۰}$	۰.۰۰۰۰۱۷	۰.۰۰۰۵۱۰	۰.۰۵۶۳۱۴	۰.۳۶۶۶۴۸	۰.۰۰۰۰۰۰۱
۶	$۱/۱ \times ۱۰^{-۱۲}$	$۱/۹ \times ۱۰^{-۶}$	۰.۰۰۰۱۱۲	۰.۰۳۱۶۷۶	۰.۲۹۹۹۸۵	۰.۰۰۰۰۰۰۱
۱۰	$۱/۰ \times ۱۰^{-۲۰}$	$۲/۹ \times ۱۰^{-۱۰}$	$۲/۶ \times ۱۰^{-۷}$	۰.۰۰۳۱۷۱	۰.۱۳۴۴۳۱	۰.۰۰۰۰۰۰۱

احتمال موفقیت مهاجم، با توجه به سهم نرخ چکیده‌سازی مهاجم و تعداد بلوک‌های عقب‌ماندگی، به‌صورت زیر محاسبه می‌شود:

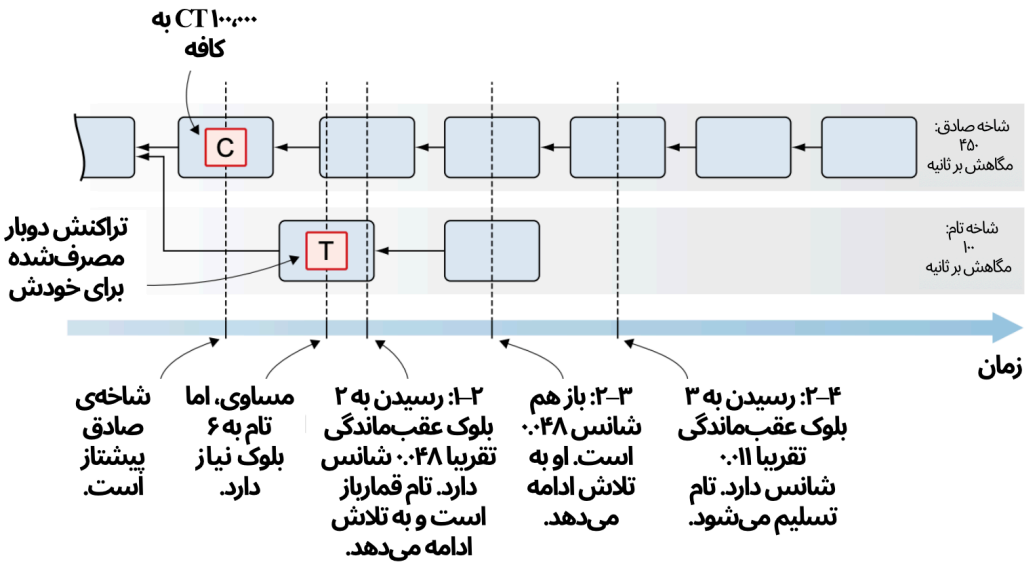
در این رابطه، q سهم نرخ چکیده‌سازی مهاجم، p سهم نرخ چکیده‌سازی استخراجگرهای درست‌کار، و z تعداد بلوک‌هایی است که مهاجم باید جبران کند:

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ \left(\frac{q}{p}\right)^z & \text{if } q < p \end{cases}$$

به ستون نرخ چکیده‌سازی ۳۶ درصد، یعنی سهم لیسا، نگاه کنید. وقتی او سه بلوک عقب است، باید در آینده چهار بلوک بیشتر از استخراجگرهای درست‌کار تولید کند. اگر حاضر باشد تا ابد تلاش کند، احتمال موفقیت او در این خرج مضاعف حدود ۱۰.۰ است. احتمالاً او نمی‌خواهد تا ابد به تلاش ادامه دهد؛ در نتیجه احتمال واقعی موفقیتش اندکی کمتر خواهد بود.

تام نیز تلاش می‌کند خرج مضاعف انجام دهد

تصور کنید تام به‌جای لیسا برای خرج مضاعف تلاش کند (شکل ۲۸.۷). او فقط نیمی از نرخ چکیده‌سازی لیسا، یعنی ۱۰۰ مگاهش بر ثانیه، را در اختیار دارد.



شکل ۲۸.۷: تام با ۱۸ درصد نرخ چکیده‌سازی تلاش می‌کند خرج مضاعف انجام دهد، اما تسلیم می‌شود. او خوش‌شانس است که تقریباً در همان زمان یافتن سه بلوک توسط استخراجگرهای درست‌کار، دو بلوک پیدا می‌کند.

شانس تام از لیسا کمتر است. او در ابتدا تا حدی خوش‌شانس است و زود دو بلوک پیدا می‌کند؛ اما پس از آنکه دو بلوک از استخراجگرهای درست‌کار عقب می‌افتد،

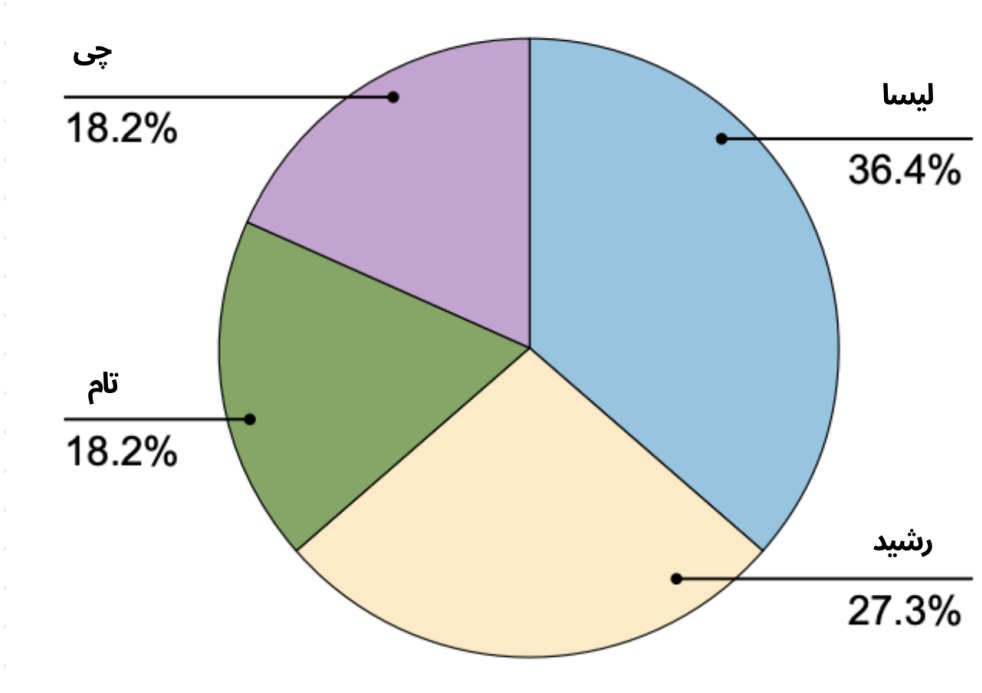
احتمال موفقیتش را بسیار پایین می‌بیند و تسلیم می‌شود. اینکه برای جبران سه بلوک عقب‌ماندگی، فقط حدود ۰۱۱.۰ احتمال موفقیت داشته باشد، فکر ناخوشایندی است.

تام فرد باهوشی است و می‌داند نباید چنین کاری را امتحان کند. او می‌فهمد که همراه با دیگران، با ایمن‌سازی بلاک‌چین و دریافت سهم منصفانه‌اش از پاداش‌ها، وضعیت بسیار بهتری دارد تا اینکه بکوشد سامانه را شکست دهد.

به‌هرحال، با ۱۸ درصد نرخ چکیده‌سازی، تقریباً یک‌پنجم تمام پاداش‌های بلوک به او می‌رسد؛ یعنی بیش از ۵۰ CT در هر ساعت. پس از ۰۰۰,۲ ساعت، یا ۱۲ هفته، او ۰۰۰,۱۰۰ توکن کلوچه را به‌صورت درست‌کارانه به دست می‌آورد، به‌جای آنکه بکوشد آن را بدزدد.

تام و لیسا برای خرج مضاعف تبانی می‌کنند

تام و لیسا در مجموع ۳۰۰ مگاهش بر ثانیه دارند و بیش از ۵۰ درصد، یعنی ۵.۵۴ درصد، از نرخ چکیده‌سازی کل را کنترل می‌کنند (شکل ۲۹.۷).



شکل ۲۹.۷: توزیع نرخ چکیده‌سازی؛ دو استخراجگر می‌توانند با تبانی، اکثریت نرخ چکیده‌سازی را کنترل کنند.

اگر آن‌ها در حملهٔ خرج مضاعف همکاری کنند و حاضر باشند تا ابد تلاش کنند،

احتمال موفقیتشان ۱۰۰ درصد است. حتی اگر فقط حاضر باشند، مثلاً، ۵۰ بلوک تلاش کنند، احتمال موفقیتشان همچنان بسیار نزدیک به ۱۰۰ درصد خواهد بود.

این سناریوی نگران‌کننده یعنی تام و لیسا می‌توانند تاریخچه را هر زمان که بخواهند بازنویسی کنند. آن‌ها از نرخ چکیده‌سازی ترکیبی همهٔ استخراجگرهای درست‌کار سریع‌ترند. می‌توانند از هر بلوکی در تاریخچهٔ بلاک‌چین شاخه‌ای ایجاد کنند، آن را تا نوک زنجیرهٔ درست‌کار پیش ببرند و از آن عبور کنند. سپس همهٔ استخراجگرها به شاخهٔ تام و لیسا منتقل می‌شوند.

توجه کنید که آن‌ها همچنان نمی‌توانند پول کسی را در بلاک‌چین بدزدند؛ اما می‌توانند هر تعداد که بخواهند خرج مضاعف انجام دهند.

فرض کنید تام و لیسا خرج مضاعف را آغاز می‌کنند. مثلاً کافه را می‌خرند و تراکنش را خرج مضاعف می‌کنند تا هم کافه و هم ۱۰۰,۰۰۰ CT را داشته باشند. هر از گاهی، مردم متوجه می‌شوند تاریخچهٔ بلاک‌چین تغییر کرده است. تراکنش‌هایی که شش تأیید داشتند، پیش‌تر قابل اتکا بودند، اما اکنون دیگر نمی‌توان به آن‌ها اعتماد کرد. اگر بلاک‌چین غیرقابل‌اعتمادتر شود، چه بر سر ارزش توکن کلوچه می‌آید؟

وقتی مردم از حملات خرج مضاعف باخبر شوند، چه بر سر ارزش توکن‌های کلوچه می‌آید؟

وحشت ایجاد می‌شود. مردم دیگر نمی‌خواهند با این سامانهٔ ناامن و غیرقابل‌اعتماد توکن کلوچه کاری داشته باشند. بسیاری از آن‌ها همهٔ توکن‌های کلوچه خود را در بازار بیرون از کافه می‌فروشند. مشکل این است که خریداران زیادی وجود ندارند. وقتی تقاضا پایین و عرضه بالا باشد، قیمت دلاری توکن کلوچه چه می‌شود؟ قیمت سقوط می‌کند.

با سقوط قیمت چه اتفاقی می‌افتد؟ وحشت بیشتر می‌شود؛ افراد بیشتری می‌خواهند بفروشند و این موضوع به افت شدیدتر قیمت منجر می‌شود.

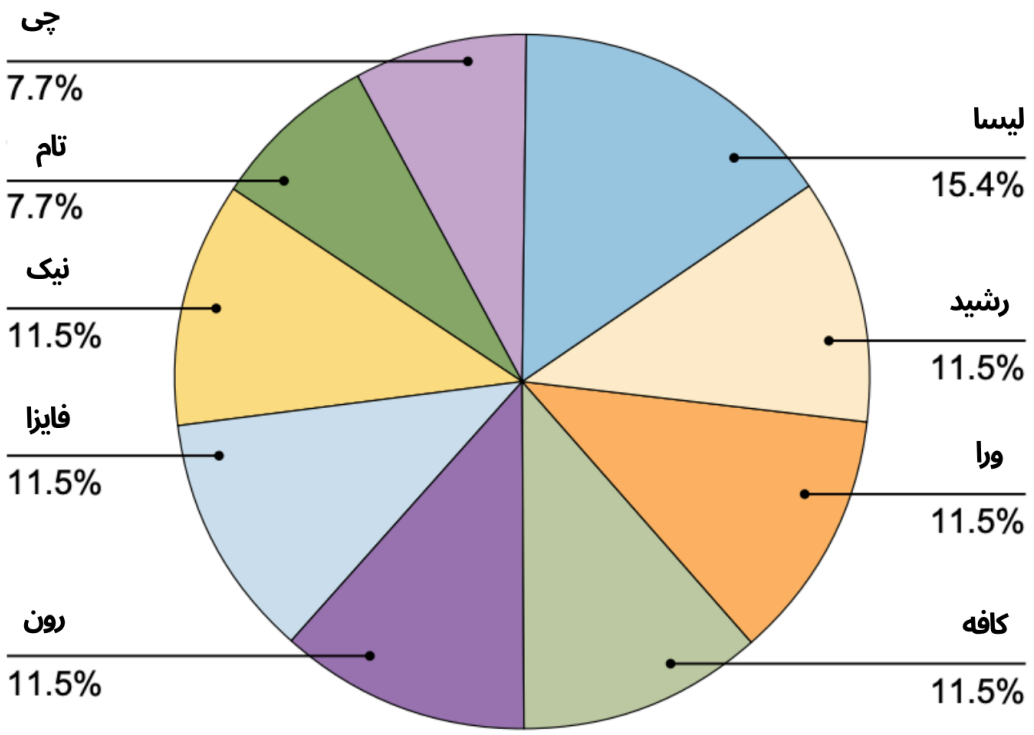
کسب‌وکار استخراج تام، لیسا و همهٔ استخراجگرهای دیگر کم‌سودتر می‌شود، زیرا ارزش پاداش بلوک آن‌قدر پایین می‌آید که نمی‌توانند توکن‌های کلوچه خود را با دلار کافی برای پرداخت قبض برق بفروشند. آن‌ها ناچارند فعالیت استخراج خود را متوقف کنند، زیرا استخراج برایشان زیان‌ده می‌شود.

تام و لیسا باید پیش از حمله به سامانه، حتی با وجود توانایی انجام آن، دوباره فکر

کنند. صرف اینکه دو استخراجگر در مجموع بیش از ۵۰ درصد نرخ چکیده‌سازی کل را کنترل کنند، می‌تواند برای ایجاد سقوط قیمت کافی باشد؛ زیرا مردم از تمرکز استخراج نگران می‌شوند؛ وضعیتی که در آن چند نفر بخش بزرگی از نرخ چکیده‌سازی کل را کنترل می‌کنند. آن‌ها حتی لازم نیست به سامانه حمله کنند تا ارزش توکن‌های کلوچه کاهش یابد.

کاهش تمرکز استخراجگرها

مردم برای مقابله با قدرت تام و لیسا چه می‌توانند بکنند؟ می‌توانند در خانه استخراج را آغاز کنند. فرض کنید پنج نفر دیگر به استخراج بپیوندند و هرکدام رایانه‌ای با نرخ چکیده‌سازی ۱۵۰ مگاهش بر ثانیه اضافه کنند. اکنون وضعیت کاملاً متفاوتی داریم (شکل ۳۰.۷).



شکل ۳۰.۷: توزیع جدید نرخ چکیده‌سازی؛ به‌دست‌گرفتن اکثریت نرخ چکیده‌سازی بسیار دشوارتر شده است.

نرخ چکیده‌سازی کل از ۵۵۰ مگاهش بر ثانیه به ۳۰۰٫۱ مگاهش بر ثانیه افزایش می‌یابد. بزرگ‌ترین استخراجگر، لیسا، با ۲۰۰ مگاهش بر ثانیه، اکنون فقط حدود ۱۵

درصد از نرخ چکیده‌سازی کل را در اختیار دارد. برای کنترل اکثریت نرخ چکیده‌سازی، دست‌کم پنج استخراجگر باید با هم تبانی کنند؛ زیرا بزرگ‌ترین چهار استخراجگر در مجموع فقط ۹.۴۹ درصد را کنترل می‌کنند.

انگیزهٔ افراد برای آغاز استخراج قوی است. آن‌ها توکن کلوچه دارند و می‌خواهند سامانه برای محافظت از دارایی‌شان در برابر سقوط قیمت ناشی از تمرکز استخراجگرها، قدرتمند باشد.

توجه کنید که با پیوستن استخراجگرهای بیشتر به رقابت، پاداش هر استخراجگر کاهش می‌یابد. در مقطعی، بعضی استخراجگرها، احتمالاً استخراجگرهای ناکارآمد، متوجه می‌شوند استخراج دیگر ارزش ندارد و رایانه‌های استخراج خود را خاموش می‌کنند. بازار، استخراجگرهای ناکارآمد را کنار می‌زند و به نفع استخراجگرهای کارآمد عمل می‌کند.

توزیع نرخ هش بیت‌کوین

در زمان نگارش کتاب، ۵۰ اگزاهش بر ثانیهٔ بیت‌کوین، بر اساس داده‌های blockchain.info، به این صورت توزیع شده بود:

این توزیع دائماً تغییر می‌کند، اما تصویری از وضعیت آن در دنیای واقعی ارائه می‌دهد.

۶.۷ کارمزد تراکنش

سامانهٔ فعلی چندین استخراجگر دارد که مستقل از یکدیگر بلوک تولید می‌کنند. این موضوع، پیشرفتی بزرگ در مقاومت در برابر سانسور است. برای جلوگیری از ورود تراکنش‌ها به بلاک‌چین، همهٔ استخراجگرها باید با یکدیگر تبانی کنند.

یک استخراجگر واحد یا بخشی از استخراجگرها فقط می‌توانند تأیید یک تراکنش را به تأخیر بیندازند. در نهایت، یکی از استخراجگرهایی که سانسور نمی‌کند، برای بلوکی شامل آن تراکنش اثبات کار معتبر پیدا می‌کند و آن بلوک را منتشر می‌سازد.

همه‌چیز خوب است، اما دو مشکل وجود دارد:

توزیع سهم نرخ چکیده‌سازی میان استخرهای استخراج.

استخر یا دسته	سهم نرخ چکیده‌سازی
BTC.com	%۱.۱۷
AntPool	%۹.۱۳
ViaBTC	%۳.۱۳
نامشخص	%۲.۱۲
Pool۲F	%۹.۱۰
BTC.TOP	%۴.۹
SlushPool	%۸.۸
Poolin	%۱.۴
BitFury	%۸.۲
DPOOL	%۳.۲
Bitcoin.com	%۷.۱
Network BitClub	%۷.۱
Bixin	%۱.۱
COIN۵۸	%۲.۰
CKPool	%۲.۰
KanoPool	%۲.۰

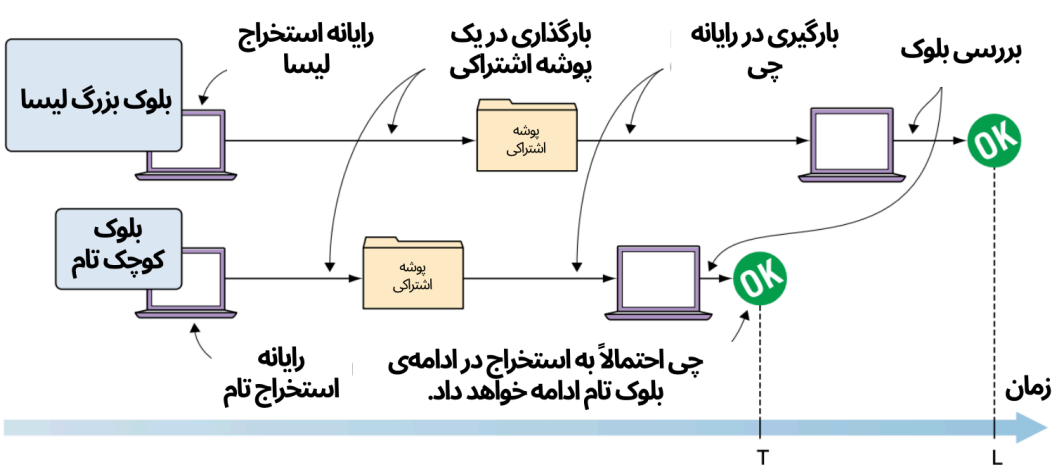
بلوک‌های بزرگ‌تر کندتر هستند.

اندازهٔ بلوک محدود است.

این دو ویژگی بر انتخاب تراکنش‌ها توسط استخراجگرها اثر می‌گذارند. ابتدا نخستین مشکل را بررسی می‌کنیم و سپس اثر محدودیت اندازهٔ بلوک را توضیح می‌دهیم.

۱.۶.۷ بلوک‌های بزرگ‌تر کندترند

فرض کنید لیسا و تام به‌طور هم‌زمان برای بلوک‌های خود اثبات کار معتبر پیدا می‌کنند. بلوک لیسا ۲۰۰ کیلوبایت و شامل ۴۰۰ تراکنش است، در حالی که بلوک تام ۱۰۰ کیلوبایت و شامل ۲۰۰ تراکنش است. هر دو می‌خواهند بلوک خودشان بخشی از قدرتمندترین زنجیره شود، اما فقط یکی از آن‌ها می‌تواند این جایگاه را بگیرد. آن‌ها دقیقاً هم‌زمان بارگذاری بلوک‌های خود در پوشهٔ اشتراکی را آغاز می‌کنند (شکل ۳۱.۷).



شکل ۳۱.۷: لیسا و تام برای ترغیب چی و دیگر استخراجگرها به استخراج روی بلوک خود رقابت می‌کنند. تام برنده می‌شود، زیرا بلوکش کوچک‌تر است.

بلوک تام از بلوک لیسا کوچک‌تر است؛ یعنی تام بلوک خود را سریع‌تر از لیسا در پوشهٔ اشتراکی بارگذاری می‌کند. دانلود بلوک تام برای چی نیز سریع‌تر از دانلود بلوک لیسا خواهد بود.

در نهایت، چی باید بلوک‌های دانلودشده را پیش از ساختن بلوکی روی آن‌ها اعتبارسنجی کند. معمولاً اعتبارسنجی یک بلوک کوچک‌تر نیز سریع‌تر از اعتبارسنجی

یک بلوک بزرگ است؛ بنابراین، اعتبارسنجی بلوک تام نیز از بلوک لیسا سریع‌تر انجام می‌شود.

در نتیجه، چی در زمان T بلوک تام را به‌عنوان نوک فعلی بهترین زنجیره انتخاب می‌کند و استخراج روی بلوک تام را آغاز می‌کند. در زمان T، بلوک لیسا عملاً برای چی وجود ندارد، زیرا چی هنوز آن را اعتبارسنجی نکرده است؛ او همچنان در حال دانلود بلوک لیسا از پوشهٔ اشتراکی است.

وقتی چی سرانجام در زمان L بلوک لیسا را اعتبارسنجی می‌کند، پیش‌تر تصمیم گرفته است روی بلوک تام کار کند. بلوک لیسا برای استفاده در سازمان‌دهی مجدد احتمالی زنجیره در آینده ذخیره می‌شود.

استخراجگرها انگیزهٔ روشنی دارند که بلوک‌های خود را کوچک نگه دارند. با هر تراکنش اضافی که وارد بلوک می‌کنند، بخشی از توان رقابتی خود را در مسابقهٔ بلوک از دست می‌دهند.

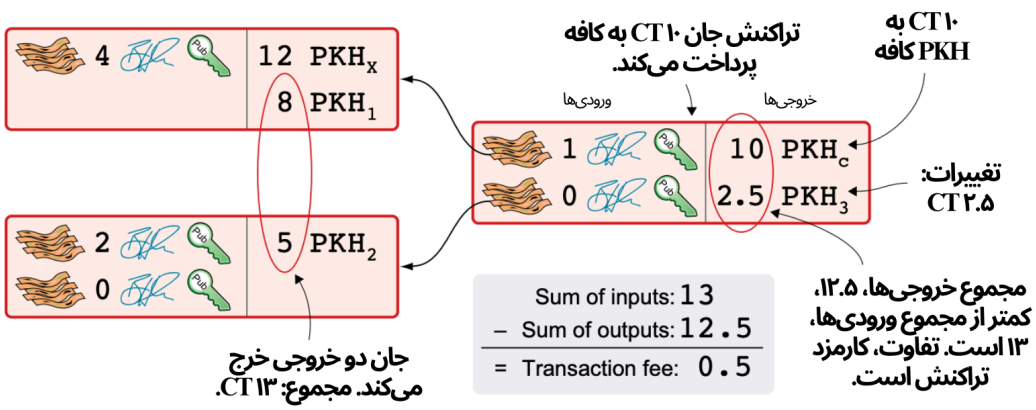
۲.۶.۷ اما موضوع، کارمزد تراکنش نبود؟

اینجاست که کارمزدهای تراکنش وارد می‌شوند. اگر استخراجگر بتواند در ازای هر تراکنشی که به بلوک می‌افزاید، مبلغ اضافه‌ای دریافت کند، این مبلغ می‌تواند کاهش توان رقابتی او را جبران کند.

افرادی که پرداخت انجام می‌دهند مشتاق‌اند تراکنش‌هایشان در بلاک‌چین تأیید شود. اگر جان بتواند مقداری پول در تراکنش خود برای استخراجگری که آن را وارد بلوک می‌کند کنار بگذارد، بسیار مفید خواهد بود. به این ترتیب، پرداخت‌کننده می‌تواند کاهش توان رقابتی استخراجگر را جبران کند.

اگر تراکنش‌ها را کمی متفاوت بسازید، می‌توانید چنین قابلیتی ایجاد کنید. فرض کنید جان می‌خواهد یک کلوچه بخرد. او برای ایجاد انگیزه در استخراجگرها جهت گنجاندن تراکنشش، کارمزد تراکنش اضافه می‌کند. او تراکنش خود را مانند شکل ۳۲.۷ می‌سازد.

وقتی جان در فصل ۵ تراکنش مشابهی ایجاد کرد، مجموع ورودی‌ها با مجموع خروجی‌ها برابر بود؛ بنابراین کارمزد تراکنش پرداخت نکرد.



شکل ۳۲.۷: جان کارمزدی برای استخراجگری که بلوک حاوی تراکنش او را استخراج کند، در نظر می‌گیرد.

این بار، جان می‌خواهد کارمزد کوچکی به تراکنش خود اضافه کند. او دو ورودی با مجموع ۱۳ CT را خرج می‌کند، یک خروجی ۱۰ CT برای کافه و یک خروجی باقی‌ماندهٔ ۵.۲ CT برای خودش می‌سازد. سپس مانند همیشه تراکنش را امضا می‌کند و آن را برای همهٔ استخراجگرها می‌فرستد.

لیسا، که یک استخراجگر است، این تراکنش را از جان دریافت می‌کند. او متوجه می‌شود که تراکنش شامل کارمزد ۵.۰ CT است. لیسا این کارمزد را می‌خواهد و تصمیم می‌گیرد کارمزد، بیشتر از آنکه کاهش اندک توان رقابتی ناشی از اضافه‌کردن تراکنش به بلوک ایجاد کند، ارزش دارد.

جان می‌تواند انگیزهٔ استخراجگرها برای گنجاندن تراکنش خود را تنظیم کند. اگر برایش مهم است که تراکنش در یکی از چند بلوک آینده تأیید شود، باید کارمزد نسبتاً بالایی بپردازد. اگر عجله‌ای ندارد، می‌تواند کارمزد کمی بپردازد؛ اما باید محتاط باشد. اگر کارمزد خیلی کم باشد، هیچ استخراجگری مایل به تأیید تراکنش او نخواهد بود.

در فصل ۹ دربارهٔ کارمزدها و افزایش کارمزد[۳۴] تراکنشی که در حالت انتظار گیر کرده است، یا «افزایش کارمزد»، بیشتر صحبت خواهد شد.

برای لیسا، هنگام تصمیم‌گیری دربارهٔ گنجاندن یک تراکنش، فقط اندازهٔ تراکنش و کارمزدی که می‌پردازد مهم است. در عمل، او به کارمزد به‌ازای هر بایت توجه می‌کند. تراکنش جان حدود ۴۰۰ بایت است و کارمزد ۵.۰ CT می‌پردازد؛ یعنی:

[۳۴] Fee bumping – معادل فارسی: افزایش کارمزد

0.00125 CT/byte

محاسبهٔ این مقدار برای لیسا ساده است و او همین کار را برای همهٔ تراکنش‌ها انجام می‌دهد. اگر کارمزد هر بایت از آستانه‌ای بالاتر باشد، تراکنش را وارد بلوک می‌کند.

او می‌تواند تراکنش‌ها را هرطور که بخواهد انتخاب کند. برای نمونه، می‌تواند تراکنش خودش را بدون کارمزد وارد کند یا همهٔ تراکنش‌های مربوط به خرید کلوچه را، صرف‌نظر از میزان کارمزد، حذف کند. این مشکلی ندارد؛ زیرا دیگر استخراجگرها روش‌های متفاوتی برای انتخاب تراکنش دارند. بیشتر آن‌ها احتمالاً فقط بر اساس کارمزد به‌ازای هر بایت تصمیم می‌گیرند.

لیسا چگونه این کارمزد را دریافت می‌کند؟ از طریق تراکنش پاداش استخراج خود (شکل ۳۳.۷).

نصف ؟CT

توکن کلوچه و بیت‌کوین را می‌توان به کسرهای بسیار کوچک تقسیم کرد. کوچک‌ترین واحد بیت‌کوین ساتوشی (Satoshi) است: هر ساتوشی برابر با $۱۰^{-۸}$ بیت‌کوین است.

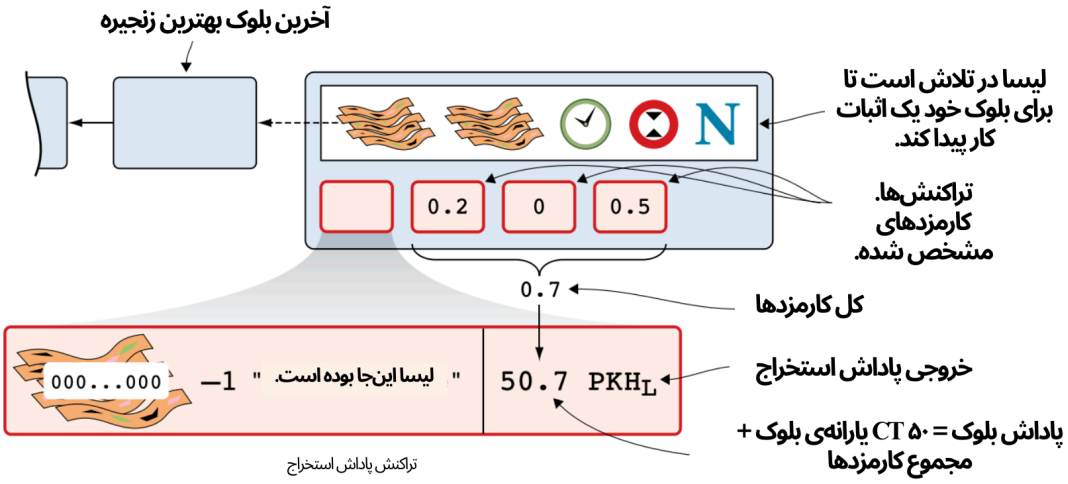
کارمزدها در بیت‌کوین

در زمان نگارش کتاب، برای آنکه یک تراکنش معمولاً در یکی از شش بلوک بعدی قرار بگیرد، کارمزدی حدود ۴ ساتوشی به‌ازای هر بایت لازم بود. هزینهٔ یک تراکنش معمولی ۵۰۰بایتی، حدود ۲۰ سنت بود.

لیسا همهٔ کارمزدهای تراکنش‌های موجود در بلوک خود را با هم جمع می‌کند و خروجی پاداش استخراج را به همین مقدار افزایش می‌دهد. مقدار موجود در خروجی پاداش استخراج، یعنی پاداش بلوک، مجموع بلوک یارانه‌ی[۳۵]، ۵۰ توکن کلوچه جدیدی که این بلوک ایجاد می‌کند، و تمام کارمزدهای تراکنش‌های آن بلوک است.

توجه کنید که اکنون معنای اصطلاح «پاداش بلوک» گسترده‌تر شده و هم بلوک یارانه‌ای، یعنی پول تازه‌خلق‌شده، و هم کارمزدهای تراکنش را در بر می‌گیرد.

[۳۵] Block subsidy – معادل فارسی: بلوک یارانه‌ای



شکل ۳۳.۷: لیسا روی بلوکی کار می‌کند که تراکنش جان و چند تراکنش دیگر را در آن گنجانده است و کارمزدها را در خروجی پاداش استخراج دریافت می‌کند.

وقتی بلوک به‌درستی آماده شد، لیسا کار برای یافتن اثبات کار معتبر آن را آغاز می‌کند.

۳.۶.۷ اندازهٔ بلوک محدود است

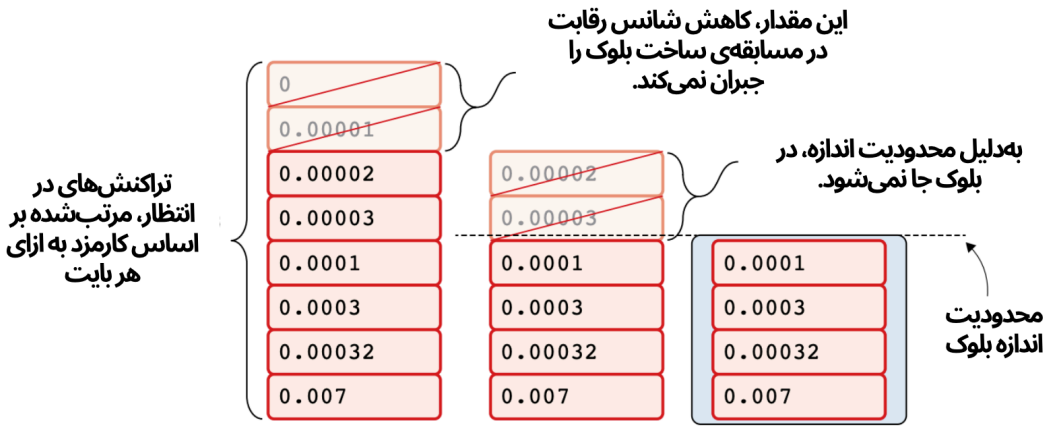
بلوک‌ها اجازه ندارند بی‌نهایت بزرگ باشند. به‌طور ساده، حداکثر اندازهٔ بلوک ۱,۰۰۰,۰۰۰ بایت است، هرچند جزئیات بیشتری از این موضوع در بخش «محدودیت اندازهٔ بلوک» از فصل ۱۰ بررسی خواهد شد.

اگر تعداد تراکنش‌های در انتظار تأیید از فضای در دسترس بلوک بیشتر باشد، استخراجگرها باید انتخاب کنند که کدام تراکنش‌ها را در بلوک وارد و کدام را حذف کنند.

کارمزد تراکنش در این وضعیت نقشی مهم دارد؛ زیرا کارمزد بیشتر، انگیزهٔ استخراجگرها برای گنجاندن یک تراکنش به‌جای تراکنش‌های دیگر را بیشتر می‌کند. افزون بر جبران کاهش توان رقابتی، کارمزد برای رقابت با تراکنش‌های دیگر بر سر فضای بلوک به کار می‌رود. این وضعیت «بازار کارمزد[۳۶]» نام دارد (شکل ۳۴.۷).

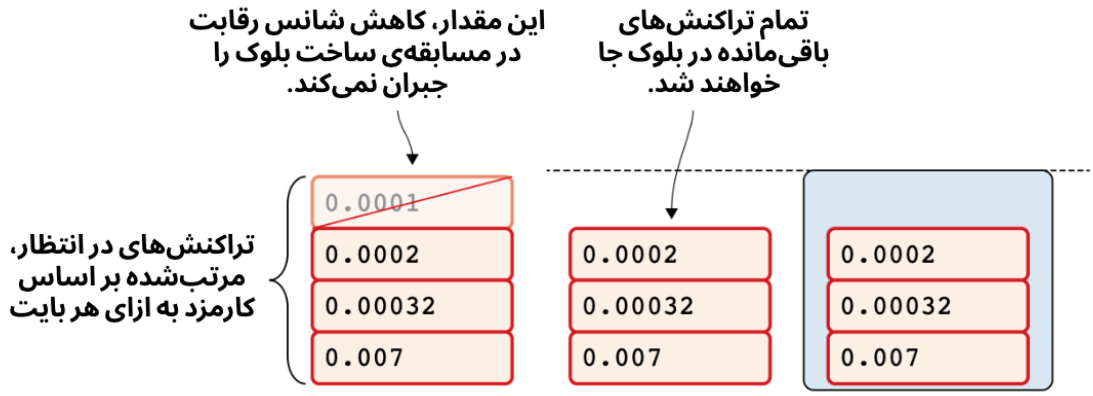
اگر فضای بلوک در دسترس از حجم دادهٔ تراکنش‌های در انتظار تأیید بیشتر باشد،

[۳۶] Fee market – معادل فارسی: بازار کارمزد



شکل ۳۴.۷: در بازار کارمزد، تراکنش‌ها بر سر فضای بلوک رقابت می‌کنند. اعداد داخل تراکنش‌ها، سطح کارمزد را بر حسب CT به‌ازای هر بایت نشان می‌دهند.

تراکنش‌ها به همان معنا با یکدیگر رقابت نمی‌کنند (شکل ۳۵.۷).



شکل ۳۵.۷: وقتی بازار کارمزد وجود ندارد، تراکنش‌ها با یکدیگر رقابت نمی‌کنند؛ فقط باید کاهش توان رقابتی استخراجگر را جبران کنند.

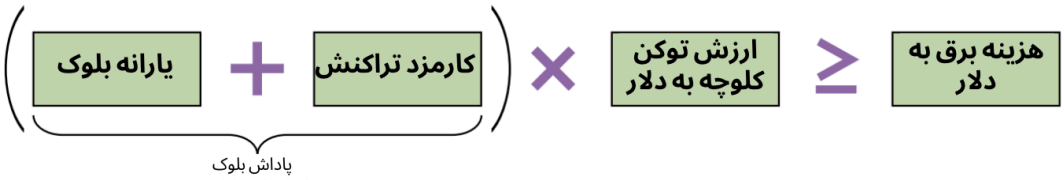
در این وضعیت، هر تراکنشی که هزینهٔ کاهش توان رقابتی را بپردازد، تأیید می‌شود.

در زمان نگارش کتاب، بازارهای کارمزد در دوره‌های افزایش ناگهانی علاقه به بیت‌کوین، گاه‌به‌گاه شکل می‌گرفتند. بااین‌حال، هنوز زمان‌هایی وجود داشت که تعداد تراکنش‌های در انتظار کم یا حتی صفر بود؛ در این حالت کارمزد پایین است و معمولاً به ۱ ساتوشی برای هر بایت، یا ۰/۰۰۰۰۰۰۰۱ BTC/byte، می‌رسد.

۴.۶.۷ وقتی یارانهٔ بلوک صفر می‌شود

همان‌طور که در فصل ۲ بحث شد، بلوک یارانه‌ای تقریباً هر چهار سال نصف می‌شود. در مقطعی، بلوک یارانه‌ای به‌تنهایی دیگر برای ایجاد انگیزه در استخراجگرها کافی نخواهد بود. اگر ارزش پاداش بلوک از هزینهٔ برق کمتر باشد، استخراج چه سودی دارد؟

با کاهش بلوک یارانه‌ای، نقش کارمزدهای تراکنش برای استخراجگرها پیوسته بیشتر می‌شود. استخراجگر معمولی می‌خواهد درآمد استخراجش دست‌کم هزینهٔ برق او را پوشش دهد (شکل ۳۶.۷).



شکل ۳۶.۷: استخراجگر باید دست‌کم به اندازه‌ای درآمد داشته باشد که قبض برق خود را پرداخت کند.

توجه کنید که ارزش بلوک یارانه‌ای لزوماً همیشه با گذر زمان کاهش نمی‌یابد. جدول ۴.۷ چند نمونه را نشان می‌دهد:

جدول ۴.۷: نمونه‌هایی از ارزش بلوک یارانه‌ای.

بلوک یارانه‌ای	ارزش ۱ CT	ارزش بلوک یارانه‌ای
CT ۵۰	۱۰.۰ دلار	۵ دلار
CT ۲۵	۲۵.۰ دلار	۲۵.۶ دلار

این جدول نشان می‌دهد بلوک یارانه‌ای به‌تنهایی معیار درآمد استخراج نیست. باید هم ارزش بلوک یارانه‌ای و هم ارزش کارمزدهای تراکنش را در نظر بگیریم. یک نکتهٔ قطعی است: وقتی بلوک یارانه‌ای صفر باشد، ارزش آن نیز صفر خواهد بود. در نهایت، بلوک یارانه‌ای دیگر انگیزهٔ کافی برای استخراج ایجاد نمی‌کند.

وقتی این اتفاق رخ دهد، کارمزدهای تراکنش برای استخراجگرهای کارآمد درآمد ایجاد می‌کنند. اگر جان بخواهد تراکنشش تأیید شود، باید کارمزدی بپردازد که برای یک یا چند استخراجگر به‌اندازهٔ کافی جذاب باشد تا تراکنش او را در بلوک خود وارد کنند. این همان بازار فضای بلوک است.

تنها می‌توان دربارهٔ سطح کارمزدها در آینده گمانه‌زنی کرد. بعضی افراد معتقدند کارمزدهای بیت‌کوین همین حالا هم برای استفاده‌ای که امروز از بیت‌کوین می‌خواهند، بیش از حد بالاست. با افزایش کارمزد تراکنش‌ها، برخی کاربردهای فعلی بیت‌کوین، مانند پرداخت‌های با مبالغ بسیار کم، باید راه‌های دیگری برای فعالیت پیدا کنند.

سامانه‌های جدیدی روی بیت‌کوین در حال توسعه‌اند که به افراد اجازه می‌دهند تعداد تقریباً نامحدودی پرداخت را فقط در یک یا دو تراکنش تجمیع کنند. یکی از این سامانه‌ها، یعنی شبکهٔ لایتنینگ[۳۷]، اهمیت ویژه‌ای دارد. اگر یک میلیون پرداخت با یک تراکنش بیت‌کوینی انجام شود، همهٔ آن پرداخت‌ها می‌توانند هزینهٔ کارمزد همان تراکنش را با هم تقسیم کنند.

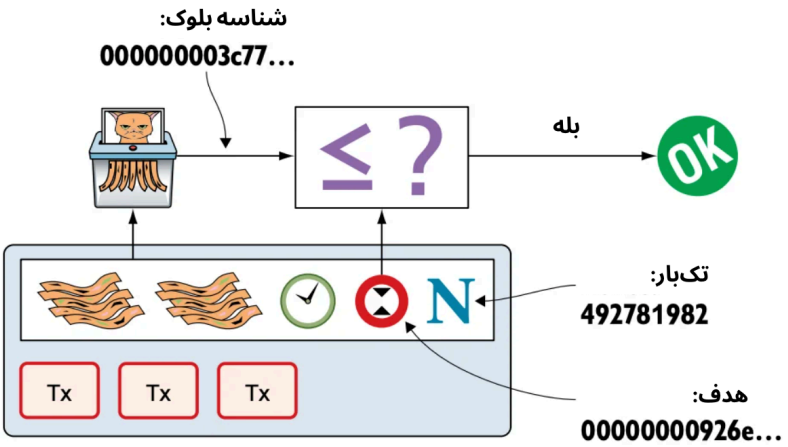
متأسفانه در این کتاب، فضایی برای پرداختن به این موضوع جذاب و پیچیده وجود ندارد.

۷.۷ مرور فصل

این فصل مسئلهٔ سانسور را حل کرد. لیسا اختیار مطلق داشت که تصمیم بگیرد کدام تراکنش‌ها وارد بلاک‌چین شوند. این مشکل را با داشتن چندین «لیسا»، یا استخراجگر، حل کردید. در نتیجه، کیف پول‌ها می‌توانند تراکنش‌های خود را برای هر یک یا همهٔ استخراجگرها ارسال کنند و امیدوار باشند برخی از استخراجگرها تراکنش‌ها را پردازش کنند.

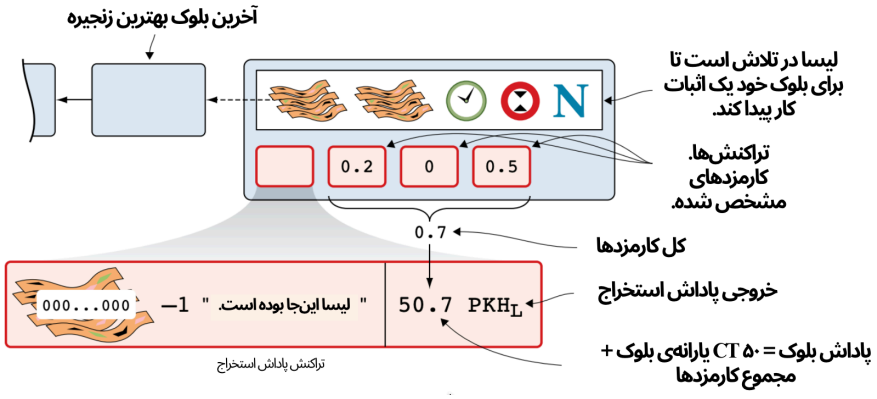
استخراجگرها برای تولید بلوک بعدی در بلاک‌چین با یکدیگر رقابت می‌کنند. آن‌ها رقابت می‌کنند تا نخستین کسی باشند که برای بلوک خود اثبات کار معتبر پیدا می‌کند.

[۳۷] Lightning Network – معادل فارسی: شبکهٔ لایتنینگ



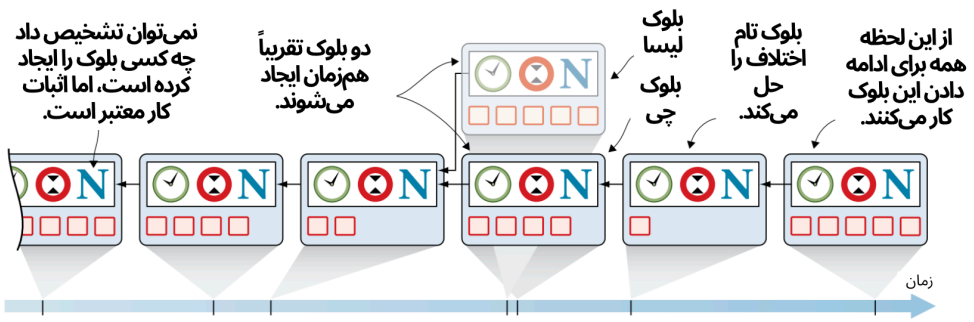
استخراجگری که در این رقابت برنده شود، بلوک خود را منتشر می‌کند و پاداش بلوک را دریافت می‌کند. این پاداش از بلوک یارانه‌ای و کارمزدهای تراکنش تشکیل شده است و در تراکنش پاداش استخراج دریافت می‌شود.

بلوک یارانه‌ای برای واردکردن عادلانهٔ پول جدید به گردش اقتصاد استفاده می‌شود تا زمانی که همهٔ ۲۱,۰۰۰,۰۰۰ توکن کلوچه جدید ایجاد شوند. فرستندهٔ تراکنش، برای ایجاد انگیزه در استخراجگرها جهت گنجاندن تراکنش در بلوکشان، کارمزد تراکنش اضافه می‌کند.

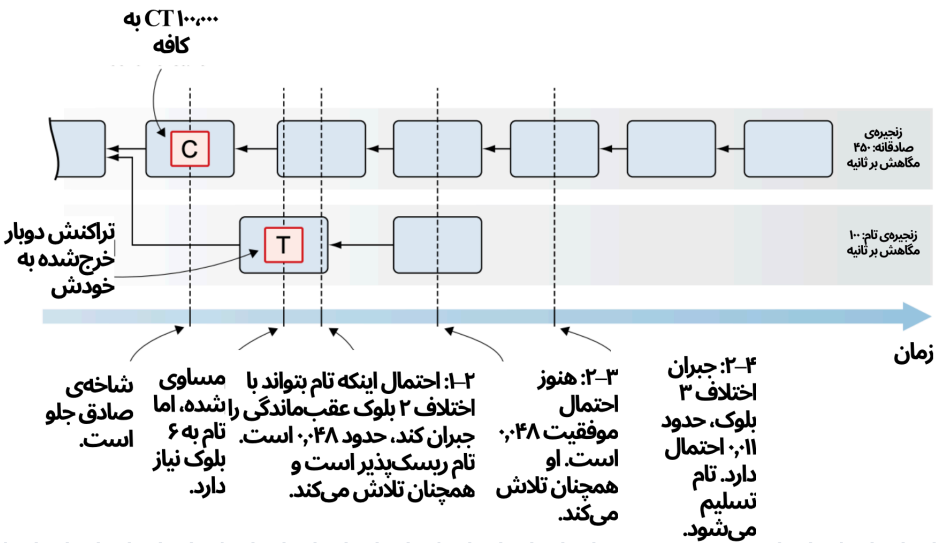


این رقابت به انشعاب‌های طبیعی منجر می‌شود؛ زمانی که دو استخراجگر تقریباً هم‌زمان یک بلوک پیدا می‌کنند. این انشعاب‌ها در نهایت حل می‌شوند.

حل انشعاب از انتخاب شاخه‌ای که استخراجگرها روی آن استخراج می‌کنند تأثیر می‌پذیرد. استخراجگرها معمولاً روی نخستین بلوک معتبری که می‌بینند استخراج می‌کنند.



یک فروشنده نباید به تراکنشی با ارزش بالا اعتماد کند، مگر اینکه تعداد کافی بلوک روی بلوک حاوی آن تراکنش استخراج شده باشد. این کار خطر خرج مضاعف را کاهش می‌دهد.



تلاش برای خرج مضاعف می‌تواند برای استخراجگر پرهزینه باشد. اگر حمله شکست بخورد، استخراجگر مقدار زیادی برق مصرف کرده و همهٔ پاداش‌های بلوک خود را از دست داده است.

انتخاب تعداد تأییدهای لازم بر عهدهٔ فروشنده است و باید ارزش تراکنش را در نظر بگیرد.

۱.۷.۷ تغییرات سامانه

اثبات کار جای امضاهای بلوک معرفی‌شده در فصل ۶ را می‌گیرد و می‌توانیم آن‌ها را از جدول نگاشت مفاهیم حذف کنیم (جدول ۵.۷). لیسا اکنون به یکی از چند استخراجگر

تبدیل شده است.

جدول ۵.۷: نگاشت مفاهیم توکن کلوچه به بیت‌کوین.

توکن کلوچه	بیت‌کوین	مطرح‌شده در
۱ توکن کلوچه	۱ بیت‌کوین	فصل ۲
لیسا	یک استخراجگر	فصل ۷
امضای بلوک	اثبات کار	فصل ۷
پوشهٔ اشتراکی	شبکهٔ بیت‌کوین	فصل ۸

لیسا اکنون دقیقاً همان وظایفی را انجام می‌دهد که یک استخراجگر بیت‌کوین انجام می‌دهد؛ به همین دلیل نام لیسا را نیز از جدول حذف می‌کنیم. پوشهٔ اشتراکی آخرین بخش از سامانهٔ توکن کلوچه است که باید به آن رسیدگی کنیم؛ این موضوع مربوط به فصل بعد است.

اکنون زمان انتشار نسخهٔ جدید و جذاب سامانهٔ توکن کلوچه است.

۸.۷ تمرین‌ها

۱.۸.۷ گرم‌کردن

۱.۷ لیسا در فصل ۶ از چه جهتی یک مرجع متمرکز بود؟

۲.۷ چرا با وجود چندین استخراجگر، یا «لیسا»، احتمال سانسور تراکنش‌ها کاهش می‌یابد؟

۳.۷ انتخاب اعداد تصادفی نسبتاً خوب کار می‌کرد، اما این ایده را کنار گذاشتیم. چرا این روش ساده‌انگارانه بود؟

۴.۷ چگونه بررسی می‌کنید که یک اثبات کار معتبر است؟

۵.۷ یک استخراجگر چگونه اثبات کار معتبر تولید می‌کند؟

۶.۷ منظور از زنجیرهٔ قدرتمندتر چیست؟

جدول ۶.۷: یادداشت‌های انتشار توکن کلوچه ۰.۷.

نسخه	قابلیت	روش تحقق
۰.۷	مقاومت در برابر سانسور	چندین استخراجگر، یا «لیسا»، که با اثبات کار فعال شده‌اند
۰.۷	هرکس می‌تواند وارد رقابت استخراج شود	تنظیم خودکار سختی
۰.۶	جلوگیری از حذف تراکنش‌ها توسط لیسا	بلوک‌های امضاشده در بلاک‌چین
۰.۶	گره‌های دارای اعتبارسنجی کامل	دانلود و اعتبارسنجی کل بلاک‌چین
۰.۵	کیف پول سبک، دادهٔ کمتری جابه‌جا می‌کند	فیلترهای بلوم و اثبات‌های مرکل
۰.۵	خرج‌کردن چند «سکه» در یک پرداخت	چند ورودی در تراکنش‌ها
۰.۵	هرکس می‌تواند تراکنش‌ها را اعتبارسنجی کند	عمومی‌کردن امضاها در صفحهٔ گسترده
۰.۵	فرستنده معیار خرج‌کردن پول را تعیین می‌کند	برنامه‌های اسکریپتی در تراکنش‌ها

۷.۷ وقتی می‌گوییم یک استخراجگر نرخ چکیده‌سازی ۱۰۰ مگاهش بر ثانیه دارد، منظور چیست؟

۸.۷ یک دورهٔ تنظیم مجدد به‌تازگی پایان یافته و تولید ۰۱۶٫۲ بلوک اخیر ۱۵ روز طول کشیده است. هدف افزایش می‌یابد یا کاهش؟

۹.۷ اگر حاضر باشید تا ابد تلاش کنید، با چه درصدی از نرخ چکیده‌سازی می‌توانید مطمئن باشید که در خرج مضاعف موفق می‌شوید؟

۲.۸.۷ مطالعهٔ عمیق‌تر

۱۰.۷ فرض کنید یک بلوک بزرگ و یک بلوک کوچک به‌طور هم‌زمان ایجاد شوند. چرا احتمال اینکه بلوک بزرگ نسبت به بلوک کوچک بخشی از قدرتمندترین زنجیره شود کمتر است؟

۱۱.۷ فرض کنید درست در میانهٔ یک دورهٔ تنظیم مجدد، نرخ تولید بلوک ناگهان دو برابر شود: به‌طور میانگین از ۶ بلوک در ساعت به ۱۲ بلوک در ساعت برسد. هیچ تغییر دیگری در طول دورهٔ تنظیم مجدد رخ ندهد. پس از پایان این دوره، چه اتفاقی برای هدف می‌افتد؟

۱۲.۷ فرض کنید سلما ۵۲ درصد از نرخ چکیده‌سازی کل را در اختیار دارد. او تصمیم می‌گیرد دورهٔ تنظیم مجدد نرم‌افزار خود را از ۰۱۶٫۲ بلوک، یعنی دو هفته، به ۱۴۴ بلوک، یعنی یک روز، تغییر دهد. هیچ‌کس دیگر این تصمیم را مناسب نمی‌داند و همه همچنان نرم‌افزار قدیمی را اجرا می‌کنند. پس از پایان دورهٔ تنظیم مجدد یک‌روزهٔ سلما و تنظیم هدف توسط او، چه رخ می‌دهد؟ آیا دیگر استخراجگرها و گره‌های کامل بلوک‌های سلما را می‌پذیرند؟ چه کسی از این وضعیت آسیب می‌بیند؟

۱۳.۷ چرا یک استخراجگر ممکن است انتخاب کند تراکنشی با کارمزد بسیار کم را تأیید نکند؟

۹.۷ خلاصه

وجود چندین استخراجگر مانع از وجود یک مرجع مرکزی می‌شود که بتواند تراکنش‌ها را سانسور کند.

اثبات کار برای انتخاب فردی استفاده می‌شود که بلوک را ایجاد می‌کند.

اثبات کار به هرکس اجازه می‌دهد بدون نیاز به گرفتن اجازه، استخراج را آغاز کند.

هدف هر ۰۱۶٫۲ بلوک به‌طور خودکار تنظیم می‌شود تا ایجاد پول با نرخ از پیش تعیین‌شده حفظ شود.

کارمزد تراکنش به استخراجگرها انگیزه می‌دهد که تراکنش را در بلوک خود قرار دهند.

برای پایین نگه‌داشتن خطر خرج مضاعف، گیرندهٔ توکن کلوچه یا بیت‌کوین تعیین می‌کند چند تأیید لازم است.

هر استخراجگر به اندازهٔ مشارکتش در نرخ چکیده‌سازی سامانه، سهمی از پاداش‌های بلوک دریافت می‌کند.

هرچه یک زنجیره قدرتمندتر باشد، یعنی اثبات کار انباشتهٔ بیشتری داشته باشد، بازنویسی آن دشوارتر است.

مراجع

[1] K. Rosenbaum. *Grokking Bitcoin*. Manning Publications, 2019.