Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۶ از ۱۳

بلاک‌ها و هش، به زبان ساده

کدهای کوتاهی که زنجیره را سر هم نگه می‌دارند، اینکه درون یک بلاک واقعاً چیست، و چرا استخراج یک بازی حدس زدن غول‌آساست

۷ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۶ از ۱۳

بلاک‌ها و هش، به زبان ساده

در یک جمله

هش کدی کوتاه است که از هر داده‌ای محاسبه می‌شود. اگر داده حتی کمی تغییر کند، کد کاملاً عوض می‌شود. هر بلاک هش بلاک قبلی را نگه می‌دارد، پس ویرایش تاریخچه قدیمی همه حلقه‌های بعدی را می‌شکند.

کدی کوتاه به جای هر داده‌ای

در درس ۳ گفتیم که هر سابقه در زنجیره، اثر انگشت دیجیتال سابقه قبلی را با خود دارد. این اثر انگشت نام مشخصی دارد: **هش** (hash).

تابع هش محاسبه‌ای است که هر داده‌ای را، چه یک کلمه، چه یک قرارداد و چه یک بلاک کامل از تراکنش‌ها، می‌گیرد و به یک کد کوتاه با طول ثابت تبدیل می‌کند. تابع هش بیت‌کوین **SHA-256** نام دارد. نتیجه آن همیشه ۶۴ کاراکتر است که از ارقام ۰ تا ۹ و حروف a تا f ساخته شده. فرقی نمی‌کند ورودی یک کلمه باشد یا یک کتابخانه کامل. نتیجه همیشه ۶۴ کاراکتر است.

هر کامپیوتری در کسری از ثانیه هش را محاسبه می‌کند، و هر کسی که همان داده را هش کند دقیقاً به همان نتیجه می‌رسد. به همین دلیل هش راهی سریع است تا بفهمیم دو نسخه از چیزی یکسان هستند یا نه، بدون اینکه خط به خط مقایسه‌شان کنیم.

با نام خودمان امتحان کنید

این هش SHA-256 متن *Market Talks* است:

`16e127cc0d60a230a1f1f80040012fc10164f835b2a99ab8f42b2ea457d9964c`

و این هش *Market talks* است، که فقط یک حرفش کوچک شده:

`79eaca857fb12aa6db2d1ab5c896ae9a3241eb2c96f99dd0640f2c6517a5a972`

یک تغییر کوچک، و هیچ چیزی در نتیجه به هم شبیه نیست. می‌توانید این‌ها را خودتان با هر ابزار رایگان آنلاین SHA-256 بررسی کنید.

چهار تضمین یک تابع هش خوب

- **ورودی یکسان، خروجی یکسان.** داده یکسان همیشه هش یکسانی می‌دهد، روی هر کامپیوتری و در هر جای دنیا.

- **تغییر کوچک، خروجی کاملاً متفاوت.** تغییر فقط یک کاراکتر کل نتیجه را به هم می‌ریزد، همان‌طور که مثال بالا نشان می‌دهد. به این **اثر بهمنی** می‌گویند.
- **فقط یک‌طرفه.** رفتن از داده به هش آسان است. برگشتن از هش به داده اصلی عملاً ناممکن است. تنها راه پیدا کردن ورودی‌ای که با یک هش جور باشد، حدس زدن بارها و بارهاست.
- **در عمل بدون تکرار.** در تئوری ممکن است دو ورودی متفاوت هش یکسانی داشته باشند، اما برای SHA-256 تا به حال هیچ‌کس چنین جفتی پیدا نکرده است. تعداد نتایج ممکن عددی ۷۸ رقمی است، تقریباً هم‌اندازه تخمین تعداد اتم‌های جهان قابل مشاهده.

این چهار قاعده در کنار هم باعث می‌شوند هش مثل یک مُهر روی داده عمل کند. اگر هش هنوز جور باشد، داده تغییر نکرده. اگر جور نباشد، چیزی عوض شده، حتی اگر فقط یک ویرگول باشد.

تشبیه: اسموتی

یک موز، کمی شیر و پنج توت‌فرنگی را در مخلوط‌کن بریزید. هر کسی با همین دستور، همین اسموتی را به دست می‌آورد. یک توت‌فرنگی اضافه کنید و طعمش عوض می‌شود. اما هیچ‌کس نمی‌تواند اسموتی را دوباره به یک موز کامل و پنج توت‌فرنگی جدا برگرداند. هش هم همین‌طور کار می‌کند: ساختنش آسان است، به هر جزء حساس است، و برگشت‌ناپذیر است.

یک بلاک چه چیزهایی دارد

یک بلاک بیت‌کوین دو بخش دارد. بخش بزرگ‌تر **بدنه** است: فهرستی از تراکنش‌ها، معمولاً چند هزار تراکنش. بخش کوچک‌تر **سرآیند** است، خلاصه‌ای کوتاه که شامل این‌هاست:

- **هش بلاک قبلی.** همین پیوند است که بلاک‌ها را به زنجیره تبدیل می‌کند.
- **خلاصه‌ای از همه تراکنش‌هایش.** تراکنش‌ها با هم هش می‌شوند و یک کد واحد می‌سازند، پس تغییر هر کدام از آن‌ها خلاصه را تغییر می‌دهد. سطح متوسط دقیقاً نشان می‌دهد این خلاصه چطور ساخته می‌شود.
- **یک مُهر زمانی** که تقریباً نشان می‌دهد بلاک چه زمانی ساخته شده.
- **هدف سختی**، که تعیین می‌کند معمای استخراج در آن زمان چقدر سخت است.
- **یک نانس** (nonce)، عددی که ماینرها هنگام جست‌وجوی یک بلاک معتبر بارها و بارها تغییرش می‌دهند. در ادامه بیشتر درباره‌اش می‌گوییم.

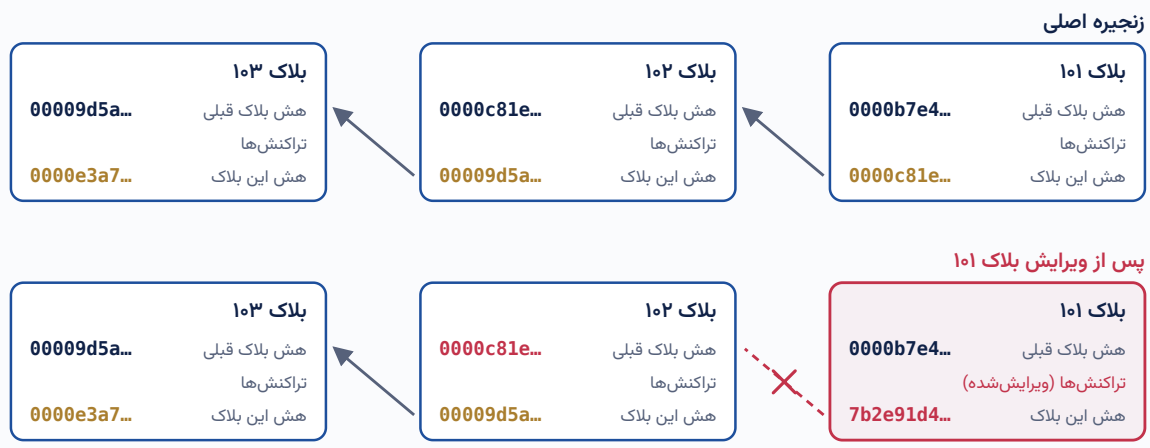
هش خود بلاک از روی سرآیندش محاسبه می‌شود. چون سرآیند هم خلاصه تراکنش‌ها و هم هش بلاک قبلی را دارد، همین یک کد به همه چیزِ درون بلاک و همه چیزِ پیش از آن وابسته است.

هش‌ها چطور زنجیره را قفل می‌کنند

حالا قطعه‌ها کنار هم قرار می‌گیرند. بلاک ۱۰۲ هش بلاک ۱۰۱ را نگه می‌دارد. بلاک ۱۰۳ هش بلاک ۱۰۲ را نگه می‌دارد. و همین‌طور تا خود بلاک پیدایش.

فرض کنید کسی فقط یک تراکنش را در بلاک ۱۰۱ ویرایش کند. خلاصه تراکنش‌هایش تغییر می‌کند، پس هشش هم تغییر می‌کند. اما بلاک ۱۰۲ هنوز هش قدیمی را نگه داشته، پس پیوند بین آن‌ها دیگر جور نیست، و هر نودی بلافاصله این را می‌بیند.

برای پنهان کردن این ویرایش، مهاجم باید بلاک ۱۰۱، بعد بلاک ۱۰۲ و بعد هر بلاکی را که پس از آن آمده دوباره محاسبه کند. و همان‌طور که بخش بعد نشان می‌دهد، ساختن هر کدام از این بلاک‌ها به حجم عظیمی از حدس زدن نیاز دارد. در همین حال، شبکه درستکار مدام بلاک‌های جدید روی آن اضافه می‌کند. به همین دلیل یک پرداخت با هر بلاکی که پس از آن اضافه می‌شود امن‌تر می‌شود.



شکل ۱. هر بلاک هش بلاک قبلی را نگه می‌دارد. ویرایش بلاک ۱۰۱ هش آن را تغییر می‌دهد، پیوندش با بلاک ۱۰۲ دیگر جور نیست، و همه می‌بینند که در زنجیره دست برده شده است.

استخراج: یک بازی حدس زدن غول‌آسا

درس ۴ گفت که ماینرها برای حل یک معما رقابت می‌کنند. این معما در واقع این است: برای اینکه یک بلاک معتبر باشد، هش آن باید از عدد هدفی که شبکه تعیین کرده کمتر باشد، که به زبان ساده یعنی هش باید با تعداد مشخصی صفر شروع شود.

چون هش‌ها یک‌طرفه‌اند، هیچ راه زیرکانه‌ای برای ساختن هشی با صفرهای زیاد وجود ندارد. ماینرها نانس را عوض می‌کنند، سرآیند را هش می‌کنند، نتیجه را بررسی می‌کنند و دوباره امتحان می‌کنند، میلیاردها بار در ثانیه. هر صفر اضافه‌ای که لازم باشد، جست‌وجو را حدود ۱۶ برابر سخت‌تر می‌کند.

ما این آزمایش را خودمان انجام دادیم: *Market Talks* را همراه با یک عدد شمارنده هش کردیم تا نتیجه با تعداد کافی صفر شروع شود:

تعداد صفر لازم	تعداد حدس‌های ما	میانگین حدس‌های مورد انتظار
۱	۱۵	۱۶
۲	۲۶۲	۲۵۶
۳	۵,۹۳۱	۴,۰۹۶
۴	۱۲۰,۵۳۹	۶۵,۵۳۶
۵	۱۲۹,۹۹۶	۱,۰۴۸,۵۷۶
۶	۱۳,۵۹۱,۱۳۰	۱۶,۷۷۷,۲۱۶

به ردیف پنج صفر دقت کنید: شانس آوردیم. استخراج یک قرعه‌کشی است و هر حدسی ممکن است برنده شود. اما به‌طور میانگین، کار خیلی سریع بزرگ می‌شود. نخستین بلاک بیت‌کوین به هشی نیاز داشت که با ۱۰ صفر شروع شود. بلاک‌های امروز به حدود ۱۹ یا ۲۰ صفر نیاز دارند، و به همین دلیل کل شبکه اکنون حدود هزار میلیارد میلیارد حدس در هر ثانیه می‌زند.

چرا این برای تریدرها مهم است

- **هر تراکنش هم یک هش دارد.** به آن **شناسه تراکنش** یا TXID می‌گویند. وقتی یک صرافی یا طرف معامله می‌گوید پرداخت ارسال شده، TXID را بخواهید و آن را در یک بلاک اکسپلورر جست‌وجو کنید. می‌بینید که آیا تراکنش وجود دارد، چه مقدار فرستاده شده و چند بلاک جدید روی آن قرار گرفته است.
- **هش‌ریت نشانه سلامت شبکه است.** هش‌ریت تعداد کل حدس‌هایی است که شبکه در هر ثانیه می‌زند. هش‌ریت بیت‌کوین نخستین بار در آوریل ۲۰۲۵ از یک زتاهش در ثانیه، یعنی عدد ۱ با ۲۱ صفر، گذشت. هش‌ریت رو به رشد یعنی ماینرها در شبکه سرمایه‌گذاری می‌کنند. یک افت ناگهانی، مثل ژانویه ۲۰۲۶ که یک طوفان زمستانی در آمریکا ماینرها را مجبور کرد بخش بزرگی از دستگاه‌هایشان را خاموش کنند، می‌تواند ماینرها را تحت فشار بگذارد.
- **ماینرهای تحت فشار ممکن است فروشنده شوند.** ماینرها هزینه برق و دستگاه‌ها را اغلب با فروش بیت‌کوین‌هایی که به دست می‌آورند می‌پردازند. وقتی درآمدشان کم می‌شود، بعضی بیشتر می‌فروشند یا دستگاه‌ها را خاموش می‌کنند. به همین دلیل بعضی تریدرها در کنار نمودار قیمت، اندیکاتورهای مبتنی بر هش‌ریت را هم دنبال می‌کنند.

اصطلاحات کلیدی

هش	کدی کوتاه با طول ثابت که از هر داده‌ای محاسبه می‌شود. داده یکسان همیشه هش یکسان می‌دهد.
SHA-256	تابع هشی که بیت‌کوین استفاده می‌کند. نتیجه‌های آن همیشه ۶۴ کاراکتر است.
اثر بهمنی	ویژگی‌ای که در آن یک تغییر کوچک در ورودی، هشی کاملاً متفاوت تولید می‌کند.
سرآیند بلاک	خلاصه کوتاه ابتدای هر بلاک. شامل هش بلاک قبلی، خلاصه تراکنش‌ها، مُهر زمانی و نانس است.
نانس	عددی که ماینرها مدام تغییرش می‌دهند تا هش بلاکی پیدا کنند که با هدف جور باشد.
هش‌ریت	تعداد کل حدس‌های هشی که شبکه در هر ثانیه می‌زند. معیاری رایج برای سنجش قدرت استخراج.

نکات کلیدی

1. هش کدی کوتاه با طول ثابت است که از هر داده‌ای محاسبه می‌شود. بیت‌کوین به SHA-256 متکی است که نتیجه‌هایش ۶۴ کاراکتر است.
2. هش‌های خوب ثابت‌اند، با هر ویرایشی کاملاً تغییر می‌کنند، برگشت‌پذیر نیستند و در عمل تکرار نمی‌شوند.
3. هر بلاک یک بدنه از تراکنش‌ها دارد و یک سرآیند که هش بلاک قبلی و خلاصه تراکنش‌هایش را در بر دارد.
4. چون هر بلاک هش بلاک قبلی را نگه می‌دارد، ویرایش یک بلاک قدیمی همه حلقه‌های بعد از آن را می‌شکند.
5. استخراج یعنی حدس زدن نانس‌ها تا هش بلاک با تعداد کافی صفر شروع شود، و هر صفر اضافه جست‌وجو را حدود ۱۶ برابر سخت‌تر می‌کند.

خودتان را محک بزنید

برای هر سؤال دور یک گزینه را خط بکشید. کلید پاسخ‌ها همراه با توضیح در صفحه بعد آمده است. این آزمون را می‌توانید به‌صورت آنلاین هم در markettalks.info انجام دهید و نتیجه را فوراً ببینید.

۱. تابع هش چه کاری انجام می‌دهد؟

A داده را رمزگذاری می‌کند تا فقط صاحبش بتواند بخواند
B هر داده‌ای را به یک کد کوتاه با طول ثابت تبدیل می‌کند
C فایل‌ها را فشرده می‌کند تا جای کمتری بگیرند
D تراکنش‌ها را در یک پایگاه داده ذخیره می‌کند

۲. یک حرف از یک سند را تغییر می‌دهید و دوباره هشش می‌کنید. چه بر سر هش می‌آید؟

A یک کاراکترش عوض می‌شود
B همان می‌ماند
C کاملاً متفاوت می‌شود
D طولانی‌تر می‌شود

۳. چرا نمی‌توان از روی یک هش به داده اصلی رسید؟

A توابع هش یک‌طرفه‌اند، پس تنها راه حدس زدن است
B شبکه هش را مخفی نگه می‌دارد
C داده اصلی پس از هش شدن پاک می‌شود
D فقط ماینرها کلید برگرداندنش را دارند

۴. چه چیزی یک بلاک را به بلاک قبلی‌اش وصل می‌کند؟

A هر دو بلاک را یک ماینر می‌سازد
B هر دو بلاک مُهر زمانی یکسانی دارند
C هر دو بلاک تراکنش‌های یکسانی دارند
D سرآیند هر بلاک هش بلاک قبلی را نگه می‌دارد

۵. نانس چیست؟

A پاداشی که ماینر دریافت می‌کند
B عددی که ماینرها هنگام جست‌وجوی هش معتبر بلاک مدام تغییرش می‌دهند
C شناسه یک تراکنش
D تعداد تراکنش‌های یک بلاک

۶. هر بار که یک صفر ابتدایی بیشتر لازم باشد، جست‌وجوی استخراج چه تغییری می‌کند؟

A دو برابر سخت‌تر می‌شود

B تغییری نمی‌کند

C حدود ۱۶ برابر سخت‌تر می‌شود

D آسان‌تر می‌شود

کلید پاسخ‌ها

۱ — B

هر داده‌ای را به یک کد کوتاه با طول ثابت تبدیل می‌کند

تابع هش از هر ورودی یک کد کوتاه با طول ثابت محاسبه می‌کند. در SHA-256، نتیجه همیشه ۶۴ کاراکتر است، اندازه ورودی هر چه باشد.

۲ — C

کاملاً متفاوت می‌شود

این همان اثر بهمنی است. هر تغییری، هر چقدر کوچک، کل نتیجه را به هم می‌ریزد و همین باعث می‌شود حتی ویرایش‌های خیلی کوچک هم به‌راحتی شناسایی شوند.

۳ — A

توابع هش یک‌طرفه‌اند، پس تنها راه حدس زدن است

هش کردن در یک جهت آسان و در جهت مخالف عملاً ناممکن است. دقیقاً به همین دلیل استخراج باید با آزمون و خطا انجام شود.

۴ — D

سرآیند هر بلاک هش بلاک قبلی را نگه می‌دارد

هر سرآیند هش بلاک قبلی را دارد. اگر یک بلاک قدیمی ویرایش شود، هشش تغییر می‌کند و دیگر با چیزی که بلاک بعدی نگه داشته جور نیست.

۵ — B

عددی که ماینرها هنگام جست‌وجوی هش معتبر بلاک مدام تغییرش می‌دهند

ماینرها نانس را تغییر می‌دهند، سرآیند را هش می‌کنند و نتیجه را با هدف و بارها بررسی می‌کنند تا هش با تعداد کافی صفر شروع شود.

۶ — C

حدود ۱۶ برابر سخت‌تر می‌شود

هر کاراکتر هش می‌تواند یکی از ۱۶ مقدار باشد، پس لازم بودن یک صفر بیشتر، نتیجه معتبر را حدود ۱۶ برابر کمیاب‌تر می‌کند.

منابع

- ساتوشی ناکاموتو، Bitcoin: A Peer-to-Peer Electronic Cash System (۲۰۰۸): https://bitcoin.org/bitcoin.pdf
- NIST، استاندارد هش امن FIPS 180-4 (SHA-256): https://csrc.nist.gov/files/pubs/fips/180-4/final/docs/fips180-4.pdf
- Forklog، عبور هش‌ریت بیت‌کوین از یک زتاهش برای نخستین بار (آوریل ۲۰۲۵): https://forklog.com/en/bitcoin-hashrate-surpasses-one-zettahash-for-the-first-time/
- KuCoin، هش‌ریت بیت‌کوین در ۲۰۲۶: روندها، سختی استخراج و امنیت شبکه: https://www.kucoin.com/blog/in-bitcoin-hashrate-in-2026-latest-trends-mining-difficulty-network-security-analysis

Market Talks

ادامه یادگیری

درس بعدی: درس ۷
نودها و شبکه همتا به همتا

این درس بخشی از دوره رایگان بلاک‌چین در مرکز آموزش MARKET TALKS است: درس‌هایی در سطح مبتدی، متوسط و پیشرفته که هر کدام یک آزمون و یک فایل PDF قابل دانلود دارند.

مرکز آموزش
درس‌هایی از اصول پایه تا موضوعات پیشرفته

تحلیل بازارها
تحلیل تکنیکال و بنیادی بازارهای اصلی

گزارش‌ها
بیت‌کوین، طلا، نقره، SPX و بیشتر

markettalks.info

تلگرام @MARKET_TALKS

•فقط برای آموزش. هیچ‌یک از مطالب این سند توصیه مالی نیست. © ۲۰۲۶ MARKET TALKS. می‌توانید این PDF را بدون تغییر به اشتراک بگذارید.