پروژه ی نرم افزار دوره کارشناسی

گزارش شماره ۶ - ماینینگ (استخراج)

آریا رادمهر - ۹۷۴۶۳۱۲۵

دکتر سجاد حق زاد کلیدبری

December 17, 2021

استخراج (Mining)

برای درک درست ماین شدن بلاک های جدید بگذارید تا دوره ای بر روی روند ساخت بلاک ها به صورت دقیق تر از قبل داشته باشیم.

بلاک ها به صورت پیش فرض میبایست:

۱- تراکنش ها (انتقالات سکه ها از یک حساب به یک حساب دیگر) توسط افراد حاضر را در خود ذخیره کنند، مادامی که نسبت به امضای درست و دوبار خرج نشدن سکه ها صحت حاصل میکنند.

۲- یک تراکنش شامل تعداد معینی سکه به خود، به عنوان پاداش در صورت پذیرفته شدن بلاک ذخیره کنند.

۳- کل تراکنش های افراد و تراکنش در صورت پذیرفته شدن بلاک را در بخش mempool ذخیره کنند.

۴- بلاکچین معتبر تا آن لحظه را نگه داری کنند.

۵- یک بلاک جدید را تحت عنوان بلاک کاندیدا (candidate block) سرهم کنند. این بلاک باید شامل هش آخرین بلاک پذیرفته شده ماقبل خود، mempool یادشده، و nonce باشد.

و در نهایت؛

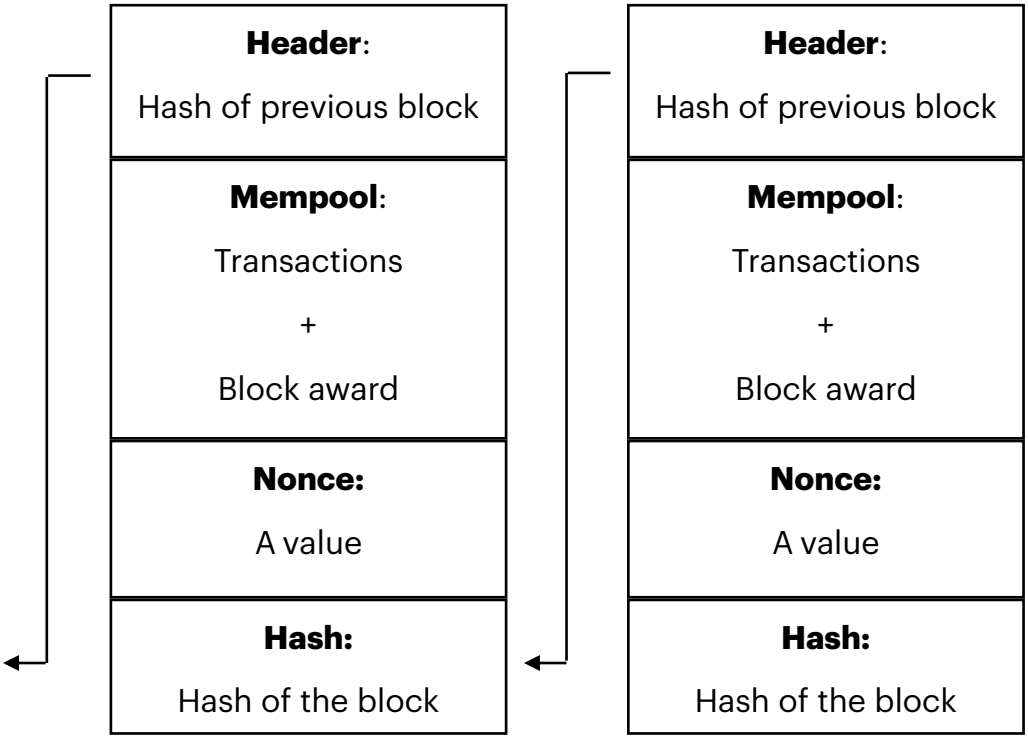
۶- به دنبال مقدار nonce ای باشند که هش محتویات کلی بلاک توسط آن، در شرط پذیرش بلاک مورد قبول واقع میشود.

به مجموع این فرآیندها ماین کردن یا استخراج میگوییم. منظور از ماینینگ به طور واضح تر، پیدا کردن nonce برای بلاک سرهم شده میباشد تا آن بلاک را توسط شرط پذیرش مورد تایید قرار دهد. در آن صورت گفته میشود که یک بلاک جدید ماین (استخراج) شده است.

Mining:

Hash (Hash of previous block, tx, tx, tx,..., Block award, Nonce)

در شکل زیر آخرین بلاک ماین شده و مورد پذیرش در بلاک چین را مشاهده میکنید.

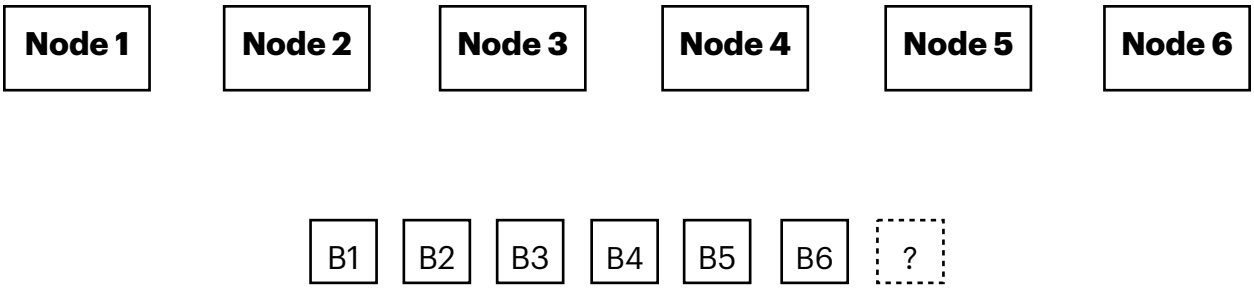


این روند به طور کلی به ازای هر بار ماین کردن بلاک های جدید طی میشود.

همانطور که بخاطر داریم سختی شبکه (difficulty level) که پیش از این با عنوان مقدار امگا (Ω) از آن یاد کردیم، تاثیر مستقیم بر روی سرعت ماین شدن بلاک های جدید دارد. اما نکته ی حائز اهمیت این است که مدت زمان ماین شدن بلاک های جدید بر روی بلاکچین باید روندی به نسبت ثابت و منطقی داشته باشد. به طوری که بلاک ها تقریبا در مدت زمان ثابتی بتوانند ماین شوند. از این رو تعیینِ مقدارِ درستِ سختی شبکه، امری بسیار حیاتی در بلاکچین ها میباشد.

حالت زیر را در نظر بگیرید.

بلاکچینی را فرض کنید که در شبکه ی آن ۶ گره به صورت مشترک مشغول به ماین کردن بلاک های جدید بر روی بلاکچین هستند.



سناریوهای زیر را تصور کنید:

۱- در حالی که ۶ گره ی در شبکه مشغول ماین بلاک های جدید هستند، یک یا چند گره به سیستم اضافه بشوند، کپی کامل بلاکچین را دریافت کرده و سپس آنها نیز مشغول ماین کردن بلاک ها بشوند.

۲- در حالی که ۶ گره ی در شبکه مشغول ماین بلاک های جدید هستند، گره ی ۲ و ۴ قدرتشان در محاسبه ی تولید هش بلاک ها (بواسطه ی افزودن سخت افزار به گره ، بهبود سخت افزار های فعلی و یا...) افزایش یابد.

۳- در حالی که ۶ گره ی در شبکه مشغول ماین بلاک های جدید هستند، یک یا چند گره از سیستم خارج شوند. (بواسطه ی نقص فنی، اتمام روند کار بر روی بلاکچین و یا...).

۴- در حالی که ۶ گره ی در شبکه مشغول ماین بلاک های جدید هستند، گره ی ۱ و ۵ قدرتشان در محاسبه ی تولید هش بلاک ها (بواسطه ی نقص فنی ، قطع ارتباط به صورت لحظه ای و یا...) کاهش یابد.

منطقی است که در سناریو های ۱ و ۲، سرعت ماین شدن بلاک ها به نسبت قبل بیشتر خواهد شد، زیرا تعداد بیشتری از گره ها بر روی ماین بلاک ها متمرکز میشوند و یا قدرت پردازش در ماین کردن بلاک ها در آنها بیشتر میشود. و یا در سناریو های ۳ و ۴، سرعت ماین شدن بلاک ها نسبت به قبل کمتر خواهد شد، زیرا تعداد کمتری از گره ها و یا سخت افزار ها مشغول به فرآیند ماینینگ میشوند. به عبارتی شانس پیدا کردن بلاک ها با سناریو های گفته شده دستخوش تغییر میشوند.

سختی شبکه باید نسبت به این تغییرات انعطاف پذیر باشد، بدان گونه که در فرآیند ماینینگ سختی شبکه باید به گونه ای تنظیم شود که بلاک ها در بازه های زمانی تقریبا منظمی ماین شده و به بلاکچین افزوده شوند. برای مثال چنانچه بلاکچین مثال بالا در مدت زمان ۵ دقیقه (به صورت متوسط) یک بلاک جدید ماین شده را به بلاکچین خود

می افزاید، در صورت رخداد سناریو های ۱ یا ۲ در شبکه، میبایست سختی شبکه بالا تر برود تا بمانند قبل بلاک ها به صورت حدودی در هر ۵ دقیقه یکبار ماین شوند. یا در صورت وقوع سناریو های ۳ و ۴ در شبکه، سختی شبکه نیز باید به همان نسبت پایین بیاید.

اما سوالی که مطرح میشود آن است که سختی یک شبکه چگونه باید محاسبه شود.

راه حل به طور مستقیم به ۲ خصوصه ی بلاکچین ما برمیگردد.

۱- مدت زمان متوسطی که میخواهیم بلاک ها ماین شوند. آنرا آلفا (α) مینامیم.

۲- تعداد بلاک هایی که میخواهیم هر بار بعد از آنها میزان سختی شبکه را بروز کنیم. آنرا بتا (β) مینامیم.

به طور کلی میتوانیم برای محاسبه ی سختی شبکه به صورت زیر عمل کنیم:

Determine Network Difficulty:

Next difficulty = (previous difficulty * α * β) / (time to mine last number of blocks)

تصور کنید بلاکچینی داریم که میخواهیم روند ماین شدن بلاک ها در آن به طور متوسط هر ۵ دقیقه یکبار باشد و همچنین مایل هستیم بعد ماین شدن هر ۱۰۰ تا بلاک، میزان سختی شبکه را بروز کنیم.

در این صورت خواهیم داشت.

Next difficulty = (previous difficulty * 5 minutes * 100) / (time to mine last number of 100 blocks)