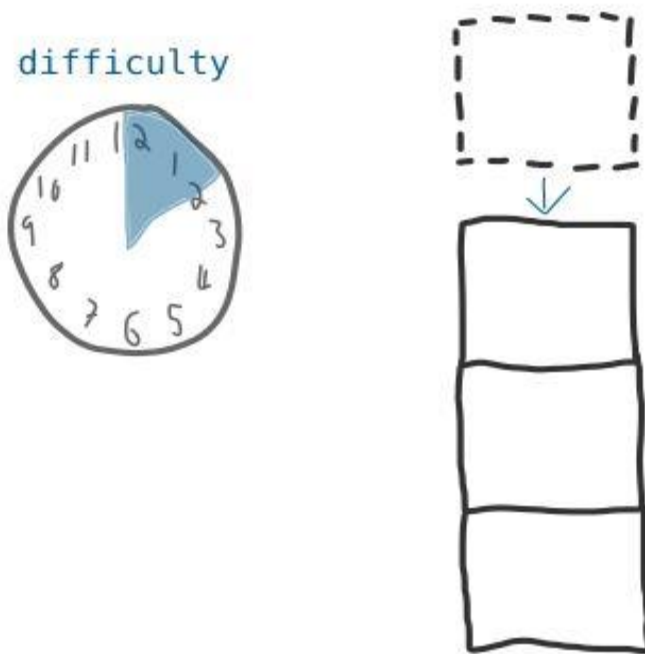


# سختی شبکه

## (برگردانده رضا تجری)

بدون اغراق می شه گفت یکی از بهترین و هوشمندانه ترین قسمت های شبکه بیت کوین فرآیند سختی شبکه و کارکرد اون می باشد.

در یک نگاه تو عکس زیر همه چی رو نشون میده که در ادامه توضیح داده خواهد شد.



سختی شبکه مقدار زمانی هست که یک ماینر بتونه یک بلاک رو استخراج کنه و بعد بلاک بعدی رو استارت بزنه برای فرآند استخراج کردن!

برای این کار یک سختی در نظر گرفته شده که ساخت این بلاک از یک زمانی بیشتر یا کمتر نشه، این سختی برای اینکه در همون بازه زمانی تعریف شده همیشه ثابت بمونه هر **2 هفته** یک بار تنظیم میشه بطوری که ساخت یک بلاک رو در بازه ثابت 10 دقیقه سعی می کنه تنظیم کنه. بنابراین تا الان متوجه شدیم که یک زمانی بین ساخت 2 بلاک داریم و اون مدت زمان 10 دقیقه می باشد (در بیت کوین) که با سختی شبکه تنظیم می شود.

## چرا سختی شبکه مهم است ؟

سختی شبکه برای این مهمه که تضمین می کنه که در هر زمان که به شبکه استخراج کنندگان چه زیاد شوند چه کم شوند توجیعه زمانی که بین ساخت هر 2 بلاک باشه به میزان 10 دقیقه انجام بگیره، ینی هرچقدر تعداد ماینرها زیاد و کم شوند سختی شبکه به تناسب آن طوری شبکه رو تنظیم می کنه که نهایتا به طور میانگین تولید هر بلاک 10 دقیقه زمان ببره. فرض کنید که اگه این سختی ثابت باشد، با اضافه شدن ماینرها میزان اضافه شدن هر بلاک کمتر می شوند.

## چه زمانی سختی شبکه تغییر می کند؟

سختی شبکه هر 2016 بلاک تغییر می کنه، که میشه همون 2 هفته یکبار، در واقع 2016 تا بلاک که میشه 2016 تا 10 دقیقه زمان باید صرف بشه که بعد زمان تغییر سختی شبکه انجام بگیره، اما یک نکته هست ما اینجا 10 دقیقه ثابت نیست، یعنی به طور میانگین 10 دقیقه می باشد، به هر حال برای محاسبه نیاز به 2016 رو ضربدر 10 (دقیقه) کنیم که به دقیقه بدست میاد، حالا اگه ماینرهای جوری استخراج کنند که میانگین 9 دقیقه بشه این زمان تغییر سختی تغییر میکنه و می شه 2016 ضربدر 9 (دقیقه).

وقتی سختی شبکه کمتر از 10 دقیقه باشه زمان ماین هر بلاک در 10 دقیقه و در وسعت 2016 بلاک، بیشتر از 1 میشه، بدین معنی که در هر 10 دقیقه یک رابطه 1.1 بوجود میاد که داره میگه در هر 10 دقیقه ما 1 بلاک و 1 دهم بلاک داریم، که از این طریق بدست میاد:

```
expected / actual  
20160 / actual
```

$$20160 / 18144 = 1.11$$

20160 برابر بوده از ضرب 10 دقیقه در 2016 بلاک که در حالت ایده آل نیاز می باشد.

18144 هم برابر هست از ضرب 9 در 2016، و نسبت دوم هم که نسبت حالت 10 دقیقه به حالت 9 دقیقه هست.

بعد از روی این نسبت میان سختی جدید رو برای شبکه تعیین می کنند که می شه رابطه زیر:

$$\text{difficulty} \times 1.11 = \text{new difficulty}$$

حالا 2 تا شرط داریم اینجا:

- اگر عدد نسبت بزرگتر از 1 باشد (به این معنی که بلاک ها سریعتر از حالت ایده آل (10 دقیقه) استخراج شده اند)، خب پس بنابراین باید سختی شبکه زیاد بشه که بتونیم شبکه رو به سمت 10 دقیقه برسونیم.
- اگر عدد نسبت کمتر از 1 باشد (به این معنی که بلاک ها کمتر از حالت ایده آل (10 دقیقه) استخراج شده اند)، بنابراین باید سختی شبکه کمتر بشه که بتونیم شبکه رو به سمت 10 دقیقه برسونیم.

و به این صورت سختی تنظیم می شه برای 2016 بلاک آینده که دوباره تا آن زمان با تعداد ماینرهای آن سنجیده خواهد شد.

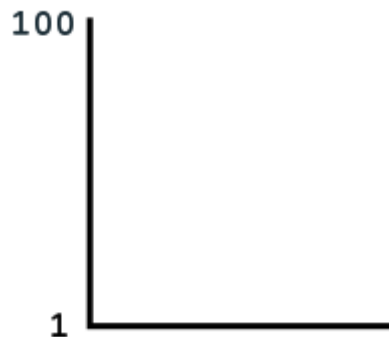
نکته: در نظر باید داشت سختی زمانی که تنظیم میشه به گونه ای هست که از یک محدوده ای بیشتر یا کمتر نمی تواند برود، به این منظور حداقل یک چهارم برابر و حداکثر 4 برابر بشه، و بیشتر از حداکثر و کمتر از حداقل ممکن نیست.

## زمان بین بلاک ها به چه شکل با سختی شبکه کنترل می شود؟

با یک مثال این قسمت رو می خوایم جلو ببریم.

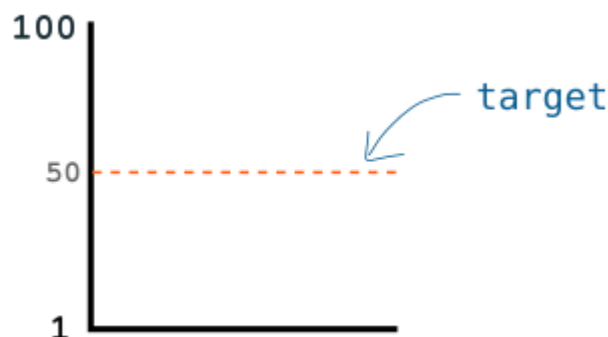
### (1) مثال ساده

فرض کنیم من به شما تعدادی از اعداد بین 1 تا 100 می دم.



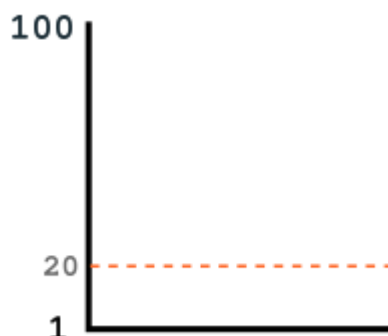
خب شما می تونید در هر دقیقه یک عدد بین 1 تا 100 بصورت تصادفی انتخاب کنید، اینقدر این انتخاب رو می تونید انجام بدید تا به عددی که من مدنظرم هست برسید.

فرض می کنیم من عدد 50 رو در نظر گرفتم.



براساس اینکه شما در هر دقیقه 1 تنها قادر به یک شماره بین 1 تا 100 هستید بنابراین این مورد 2 دقیقه زمان می برد.

اما این خیلی آسونه، بنابراین هدف رو به 20 تغییر می دم، حالا شما می توانید هر 1/5 امتحان کنید، یا به معنی اینکه هر 5 دقیقه یک بار بدست بیاورید.

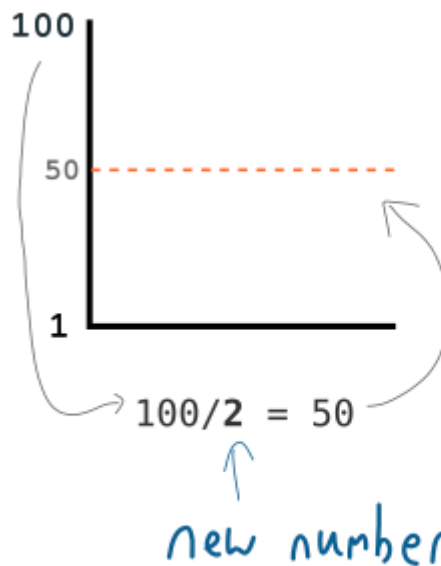


یک نکته ای که هست شاید شما بار اول که عدد رو انتخاب می کنید خوش شانس باشید و مستقیماً 20 رو انتخاب کنید، ولی در بلند مدت به همان 5 دقیقه خواهید رسید و ینی به صورت هر 5 دقیقه به این شرایط می انجامد.

بنابراین بر اساس میزان انتخابی که شما می توانید انجام دهید، می توانید از مقدار هدف استفاده کنید برای اینکه چه میزان زمان طول بکشد تا عدد مورد نظر بدست بیاید.

## معرفی سختی شبکه

در اینجا سر و کار با کامپیوتر هست و کامپیوتر می تونه بجای اینکه به طور مستقیم به هدف اشاره کنه بیاد اون رو به تقسیماتی از محدوده ای از اعداد تقسیم کنه و از دل اون اعداد جدیدی بدست بیاره که نهایتاً به جواب یا هدف مسئله برسه.

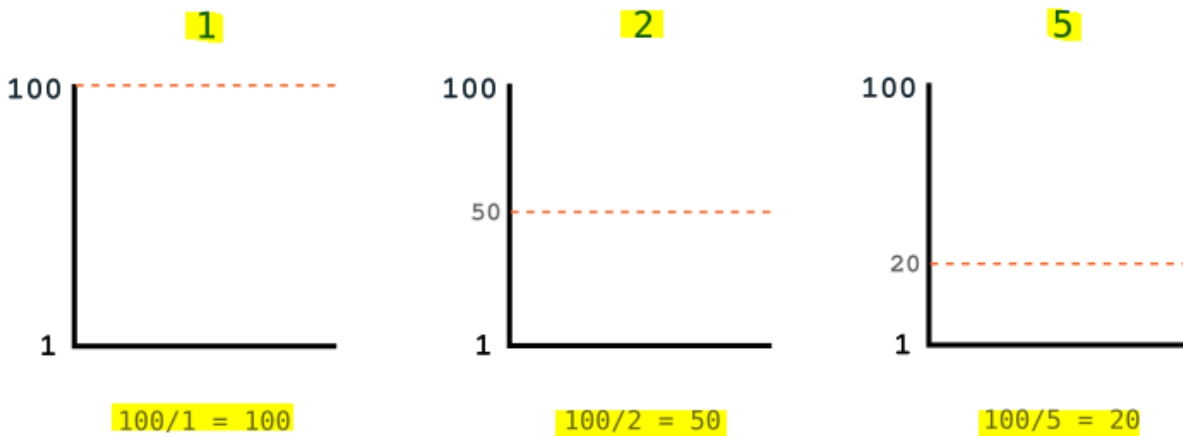


This new number is able to control the height of the target.

این شماره جدید همان سختی شبکه می باشد، که درواقع خیلی ساده می شه از اون استفاده کرد برای تغییر مقدار عدد مورد نظر و بتناسب اون طول زمان مورد نظر، تمام این فرآیند در یک رابطه زیر نشان داده شده است:

$$\text{target} = \text{targetmax} / \text{difficulty}$$

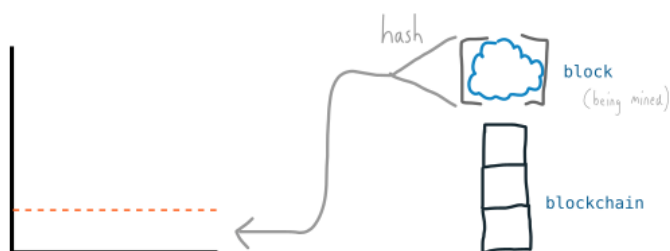
نمونه های مختلفی رو برای مثال در زیر میبینیم که با تغییر سختی شبکه چطور طول پیدا کردن هدف رو سخت تر می شه کرد:



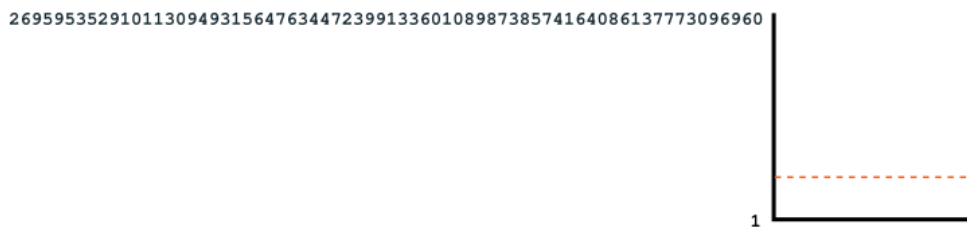
The higher the difficulty, the lower the target.

## (2) مثال بیت کوین

برای بیت کوین همانند مثال ساده که در قبل بود کار می کنه، به این منظور فرآیند هشینگ کاندید بلاک انجام میگیره تا ماینرها بتونن بهترین شانس های خودشون رو امتحان کنند تا به عدد مورد نظر برسند، در اینجا ماینرها امیدوارند که محدوده بازه ای کمتری رو بتونن انجام بدن که سریعتر به عدد مورد نظر برسند.



And seeing as miners are able to generate thousands of numbers (hash values) per minute, bitcoin uses ridiculously big numbers.



The numbers in bitcoin are just on a much bigger scale.

14484.162361

26959535291011309493156476344723991336010898738574164086137773096960

1861311315012765306929610463010191006516769515973403833769533170

1

not to scale

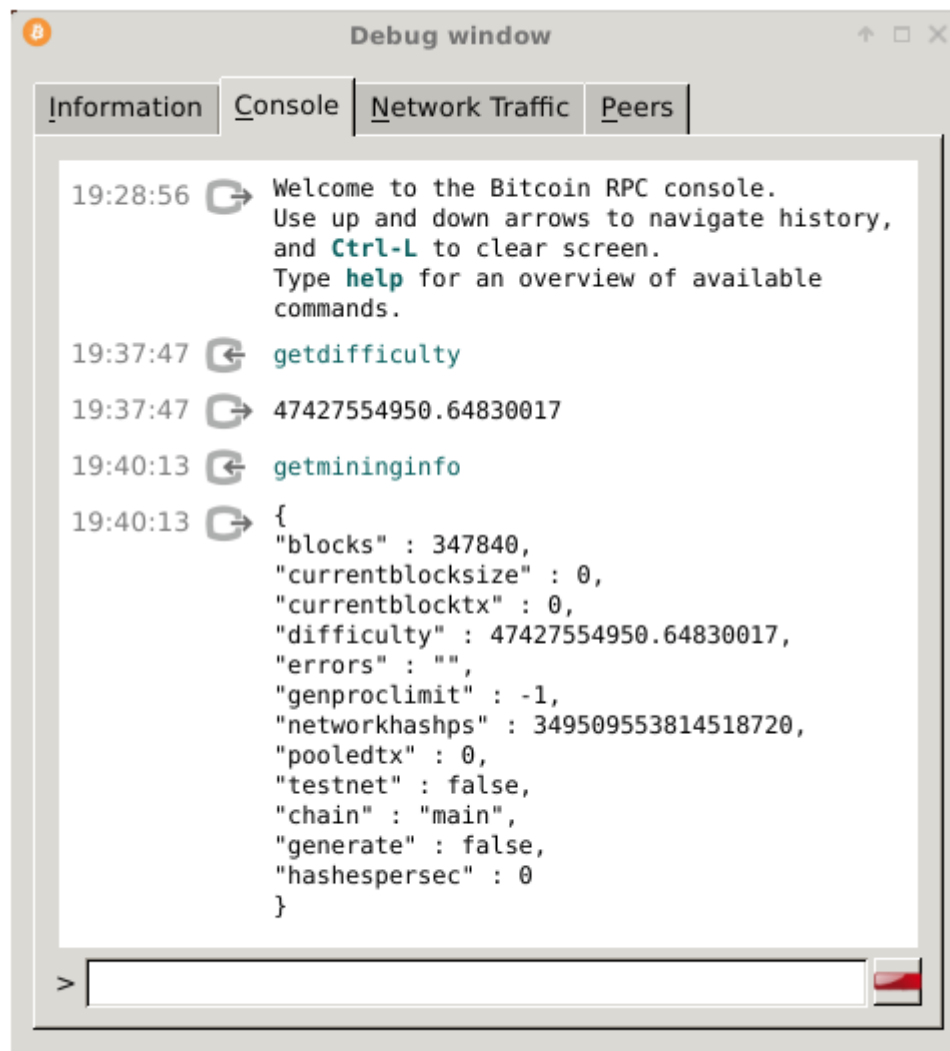
## معرفی اعداد هگزادسیمال

(still not to scale)









با اینحال اگر شما یک کلاینت از بیت کوین را ندارید و نیستید، می توانید سختی شبکه را همیشه از آدرس زیر پیدا کنید:

<http://chainquery.com/bitcoin-api/getdifficulty>

و همینطور اگر علاقه مند هستید که سختی شبکه در طول زمان چگونه تغییر می کند، می توانید از وبسایت زیر استفاده کنید که به همراه چارت هم می باشد:

<https://bitcoinwisdom.com/bitcoin/difficulty>

Source: <http://learnmeabitcoin.com/guide/difficulty>

لذت ببریم از تکنولوژی !

تموم شد./شاد زی..