کلید خصوصی

(برگردانده رضا تجری)

یک کلید خصوصی چیست ؟

یک کلید خصوصی یک عدد می باشد که به صورت تصادفی ایجاد می شود.

به عنوان مثال یک نمونه از کلید خصوصی شبیه زیر می باشد:

```
108165236279178312660610114131826512483935470542850824183737259708197206310322
```

به صورت دقیق تر اگه بخوایم برای بیت کوین بگیم، به این صورت است که از شماره هایی بر اساس 256 بیتی استفاده میشه که به صورت تصادفی ایجاد می شن:

برای مثال (حالی دودویی "باینری")

```
1110111100100011010110101010110011111001000011011001111101001010101010110
1110110001100100100101110010010110010010101100010111000011101100111101
1110010111111100001101111110011011101000111011010100001000001001011000
1110011100111001011000000010011110110110010
```

این یک عدده، ولی به صورت دودویی هستش که یک روش ذخیره اعداد به کامپیوتر می باشد، و
همینطور که می دونید بیت کوین در نهایت یک برنامه کامپیوتری هستش، کامپیوتر هم که صفر و یک !

با این حال می می تونیم به راحتی این عدد دودویی رو به دسیمال (دهدهی) تبدیل کنیم:

```
108165236279178312660610114131826512483935470542850824183737259708197206310322
```

یا به شکل هگزادسیمال:

```
ef235aacf90d9f4aadd8c92e4b2562e1d9eb97f0df9ba3b508258739cb013db2
```

همه این شکل ها یکی هستند و هیچ تفاوتی بین اونها نیست و درواقع همه اون ها کلید خصوصی یکسانی رو نشان می دهند، ولی در شکل های گوناگون، نتیجه می گیریم که یک کلید خصوصی تنها عدد می باشد !

معمولا کلید خصوصی رو به صورت هگزادسیمال نشون میدن.

شماره های 256 بیتی چیست ؟

یک شماره ای که 256 بیت باشه توانایی این رو داره که 256 بیت از داده رو ذخیره کنه.

بیت چیست ؟

کوچیکترین واحدی که در کامپیوتر می باشد بیت نامیده می شود.

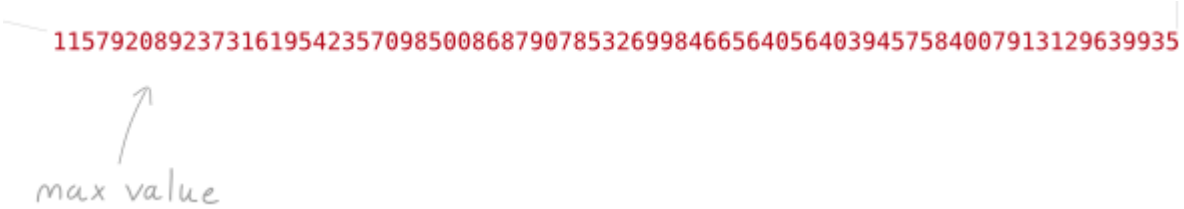
Unit	Size
gigabyte	1024 megabytes
megabyte	1024 kilobytes
kilobyte	1024 bytes
byte	8 bits
bit	

درواقع یک بیت خیلی کوچیکه و تنها می تونه مقادیری مثل 0 یا 1 رو در خودش نگهداری کنه.

با این حال، همین بیت ها نشان دهنده از نوعی داده در کامپیوتر می باشند، همچون اعداد روزمره که بکار می روند.

برای مثال در اینجا؛ چگونگی ذخیره شدن چند عدد مختلف در کامپیوتر را نشان می دهیم:

به هر حال یک عدد 256 بیتی یک عدد ساده ای می باشد که می تواند به اندازه 256 عدد (حداکثر) نمایش داده شود.



یا به عبارت دیگه یک عدد 256 بیتی هست بین:

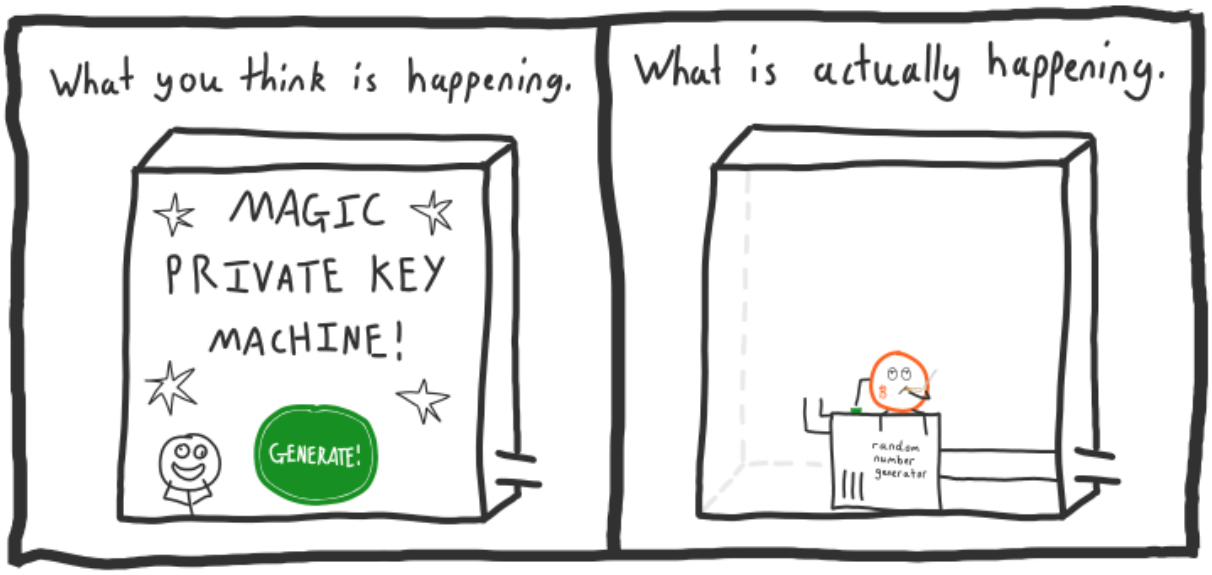
```
min: 0
max: 115792089237316195423570985008687907853269984665640564039457584007913129639935
```

بنابراین همانطور که می بینیم یک 256 بیتی به شما یک فضای بزرگی از اعداد می دهد که می توانید از ان استفاده کنی، و این همه همان 256 بیت هستش، اعدادی که شامل 256 بیت از داده را شامل می شوند.

تعدا کل 256 عدد بیت برابر است با عدد 2^256.

کلید خصوصی از کجا می آید ؟

من دروغ گفتم وقتی که داشتم می گفتم کلید خصوصی به صورت تصادفی ایجاد میشه !!
صادقانه بخوام بگم، زمانی که شما از هر نوعی نرم افزار تولید کلید خصوصی برای بیت کوین استفاده کنید، اونها جادویی برای شما انجام نمیدن، آنها به شما فقط یک شماره 256 بیتی که به صورت تصادفی هست می دهند.

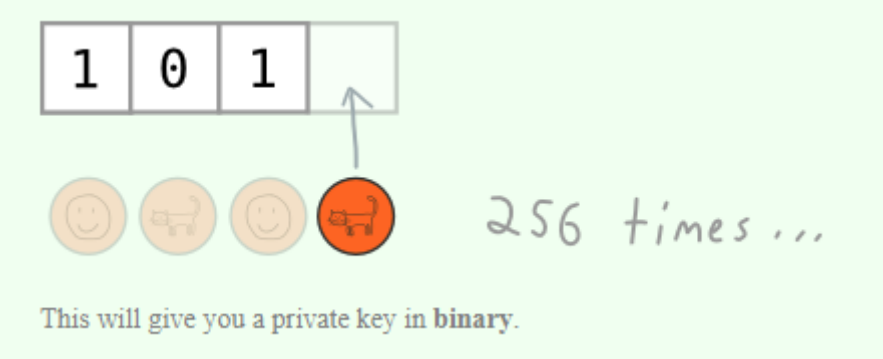


بنابراین، هیچ دلیلی وجود نداره که شما نتونید کلید خصوصی خودتون رو ایجاد نکنید، همه شما نیاز به این دارید که توانایی داشته باشید یک شماره تصادفی 256 بیتی ایجاد کنید.

به چندین روش مختلف میتونی این کارو انجام بدی:

مثال

1. 256 بار سکه بندازی

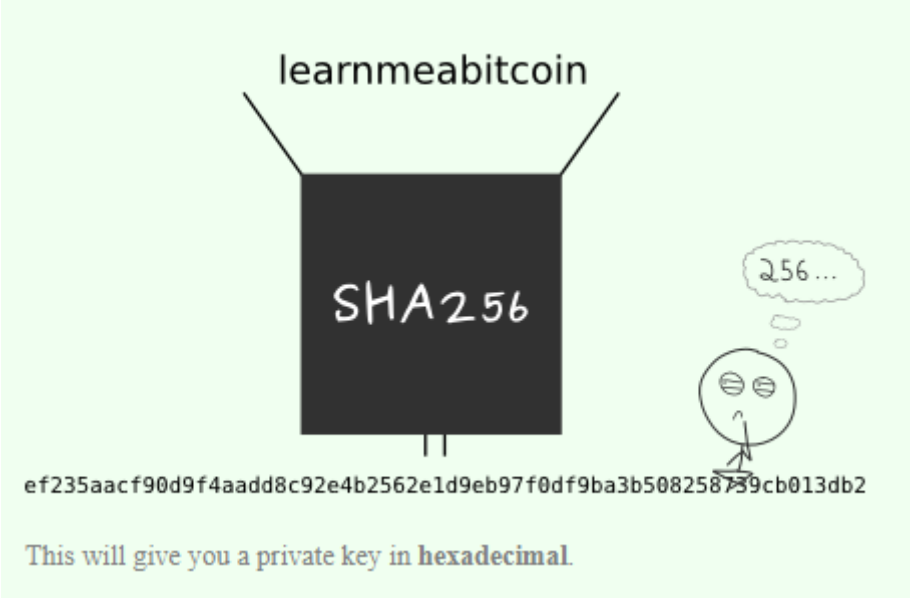


2. از یک زبان برنامه نویسی مورد علاقه ای که دارید برای تولید عدد تصادفی استفاده کنید.

```python
# need to use the operating system's random number generator for security
import random
random.SystemRandom().randint(1, 115792089237316195423570985008687907852837564279074904382605163141518161494337)
```

This will give you a private key in **decimal**.

بعضی از این هش ها از تابع هش SHA256 استفاده می کنند.



تمامی این روش ها به شما یک عدد تصادفی 256 بیتی می دن، و اگه شما یک شماره 256 بیتی گرفته باشید، شما یک کلید خصوصی گرفته اید.

مطمئن بشید که شماره ای که گرفتید به صورت کاملا تصادفی ایجاد شده باشد. [1]

اگه از یک جایی که مطمئن نباشید خروجی که می ده یک عدد کاملا تصادفی نیست، (برای مصال در الگوهایی که برای تولید عدد تصادفی هستند)، شما خودتون رو در معرض خطر و آسیب پذیری قرار دادی به جهت کلید خصوصی، زیرا از منبعی برای ایجاد عدد تصادفی استفاده کرده اید که کاملا تصادفی نبوده.

و درواقع اگه کسی توانایی بازیابی کلید خصوصی شما رو داشته باشه می تونه به بیت کوین های شما دسترسی داشته باشه.

در نتیجه، تمامی این راهنمایی هایی که مدام تاکید می شه و به نوعی شما رو می ترسونند از بابت تولید کلید خصوصی برای اینه که کسی مسئول خطاهای تازه واردانه شما نمی تونه باشه، بنابراین بسیار در این مسئله دقت کنید که مبادا از منبعی بی اعتبار کلید خودتون رو دریافت کنید.

اگه کسی می بینید به این مسائل زیاد دقت نمیکنه شما توجه نکنید، در این مسئله سهل انگاری نکنید، و تا جایی که می تونید محکم کاری کنید بگذارید هر کسی توجهی و بی دقتی داره، برای کلید خصوصی خودش این نگه رو داشته باشه.

با قرار دادن کلمه "bitcoin" در تابع هش SHA256 (به جهت استفاده برای کلید خصوصی)، این هست خیلی خنده دار برای اینکه فک کنید یک کلید خصوصی تصادفی ایجاد کرده اید.

اگه شما هنوز مطمئن نیستید، 256 بار یک سکه رو بندازید، شما نمی تونید حالت تصادفی تری از این حالت بگیرید.

این واقعیت که هر کسی می تونه ایجاد کنه حساب بیت کوین خودش رو اونم توسط یک عدد که به صورت تصادفی ایجاد می شه، این هست یک ویژگی دوست داشتنی برای بیت کوین، این به این معنیه که هیچ کسی کنترلی بر روی صدور حساب ها نداره، بنابراین بیت کوین برای هر کسی که بخواد به صورت باز (آزاد) قابلیت ایجاد کردن شماره 256 بیتی رو داره.

اگه یک فرد دیگه مثه کلید خصوصی من ایجاد کنه، اونوقت چی !؟

اگه این اتفاق بیوفته، اون فرد توانایی این رو داره که بیت کوین های شما رو به سرقت ببره.

اما نگران نباشید، هیچ کسی نمی تونه به صورت تصادفی کلید خصوصی مثل کلید خصوصی شما ایجاد کنید.

آیا واقعا اونها می تونن ؟

ببینید بدست آوردن کلید خصوصی ممکن هست، اما با توجه به گستره وسیعی که برای کلید خصوصی هست این کار به شدت سخت هست و درواقع اینقدر این کار مشکل هستش، که "بعید" محسوب میشه.

برای مثال اگه من یک میلیون میمون داشته باشیم، که در هر ثانیه میلیون ها کلید خصوصی ایجاد کنند (در حالتی که به اونها خوب هم آموزش داده شده باشه) یک چیزی شبیه این میشه:

3,671,743,063,080,802,746,815,416,825,491,118,336,277,193,184,902,172 سال **[2]** طول می کشه که کلید خصوصی مثل شما ایجاد بشه، ببینید این اعداد نشان دهنده سخت بدست اومدن کلید خصوصی شبیه به کلید خصوصی شما هست، که فقط بدونید این کار به شدت سخته.

برای همین کلید خصوصی که کاملا به صورت تصادفی انتخاب شده هست بسیاری خصوصیت درون خودش داره که از امنیت بالایی برخوردار می شه.

نمایش کافی

محدوده ی (گستره ی) 256 بیت شماره (و نتیجتا شماره هایی که ممکنه کلید خصوصی باشند) خیلی بیش از حد بزرگ هستند، همانطور که برای ذهن انسان غیر ممکنه (خیلی سخت) هستش که مقسای جهان رو تصور کنه، در اینجا هم ذهن انسان برای تجسم گستره ی 256 بیت دشواری داره و غیر ممکن است که بتونه همچین رنج از اعداد رو تصور کنه.

بنابراین اگه شما هر نوع تردیدی برای ایمنی 256 بیت از شماره خودتون داشتید، این به این دلیله که شاید شما از یک تولید کننده مناسب که به صورت تصادفی بوده باشه استفاده نکردید و یا اینکه نمی دونید با چه حجم بزرگی از اعداد و محاسبات در این قسمت روبرو هستیم که متوجه بشید با سختی زیادی طرف هستیم.

پاورقی

1. هیچ چیزی کاملا تصادفی نیست، اما همیشه باید بهترین ها رو انتخاب کنید
2. نحوه محاسبه مدت زمان بالا

```python
keys = 115792089237316195423570985008687907852837564279074904382605163141518161494337
monkeys = 1000000
monkeyhashrate = 1000000

keyspersecond = monkeys * monkeyhashrate

seconds = keys / keyspersecond
minutes = seconds / 60
hours = minutes / 60
days = hours / 24
years = days / 365
millionyears = years / 1000000

print millionyears
```

Source: http://learnmeabitcoin.com/guide/private_keys

کلید خصوصی حُکم پول نقد توی دستاتون رو داره، اگه کلید خصوصی رو به جای تحویل بدید مثه این میمونه که پول نقدتون رو به اون جا سپردین.

شاد زی.