کلید عمومی

(برگردانده رضا تجری)

یک کلید عمومی چیست ؟

یک کلید عمومی شکل اولیه ای از یک آدرس هستش، و همانند کلید خصوصی به صورت هگزادسیمال ذخیره می شود، مثال:

```
public_key  = 02b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a8737
```

به هر حال جالبه که بدونید کلید عمومی شما از **روی کلید خصوصی شما** ایجاد شده است.

اگه این شکل از کلید عمومی رو فشرده سازی به شکل کوتاه تر (که در این حالت آدرس نامگذاری می شه) نکنیم، همچنان می توانیم از کلید عمومی برای آدرس حساب استفاده کنیم برای اینکه مثلا بیت کوین ارسال بشه به این آدرس.

چگونه یک کلید خصوصی از روی کلید عمومی بدست می آید ؟

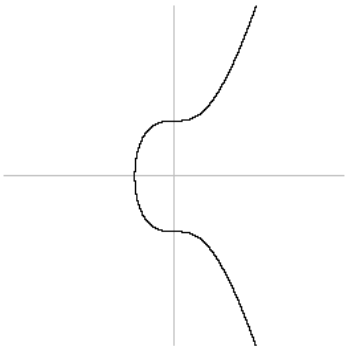
شما با قرار دادن کلید خصوصی خودتون به یک تابع خاص ریاضی می توانید کلید عمومی مربوط به کلید خصوصی خودتون رو دریافت کنید.

یک تابع چیست ؟

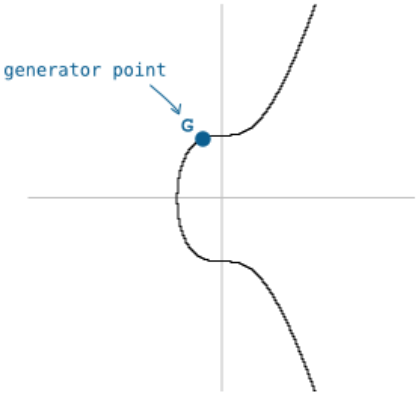
این تابع خاص رو منحنی بیضوی می نامند، که اساسا در بر میگیره اطراف این منحنی رو روی نمودار تا زمانی که به خروجی نهایی که طبق تابع مورد نظر انجام می گیرد برسد که در نهایت برای شما کلید عمومی رو بوجود بیاره! به شکل زیر توجه کنید.

منحنی بیضوی شکل به چه شکل می باشد ؟

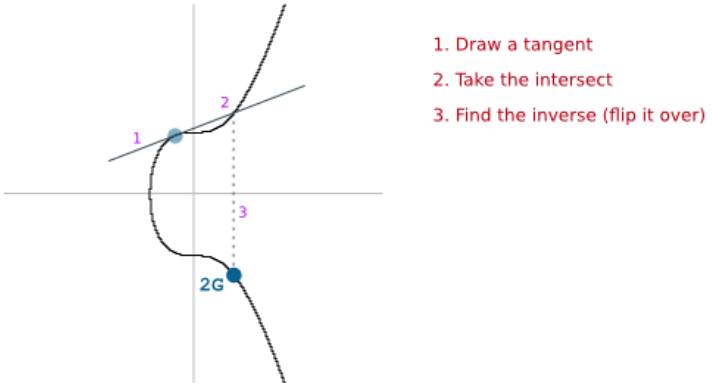
شبیه شکل زیر:



علاوه بر این، منحنی بیضوی در بیت کوین دارای نقاط شروع خاصی می باشد.



اگه ما در این نمودار عملیات ضرب انجام می دادیم (به عنوان مثال نقطه را در 2 ضرب کنیم)، ما می توانیم حرکت کنیم در اطراف منحنی.



The fact that we can draw a tangent anywhere on the curve and it will intersect *one* other point on the curve is a special feature of elliptic curves.

و حالا ما اون رو در اختیار داریم، ما فقط مختصات نقطه (G) رو در 2 ضرب کردیم و مختصاد نهایی (2G) رو پیدا کردیم.

این درواقع حاصل یک دور از ضرب شدن در منحنی بیضوی است.

نکته ای رو بدونیم که این کلمه "ضرب" در اینجا حالت عادی ای از ضرب نیست و حالت خاصی می باشد که به عنوان ضرب در نظر گرفته ایم !

اگه شما 2 را در مختصات G ضرب کنید حاصل مختصات 2G را نمی دهد (همانطور که در نمودار نشان داده شده است).

درواقع رسیدن به این مختصات از روشی هوشمندانه بدست میاید که اون رو یک عنوانی باید نامگذاری کرد، که از کلمه "ضرب" استفاده گردیده است.

زیرا همانطور که می دونید، ریاضیات می تونه هرگز به اندازه کافی گیج کننده نباشه.

بنابراین زمانی که ضرب را از این به بعد بکار بردیم منظور ما "ضرب منحنی بیضوی" می باشد.

چگونه یک کلید عمومی بدست می آورید ؟

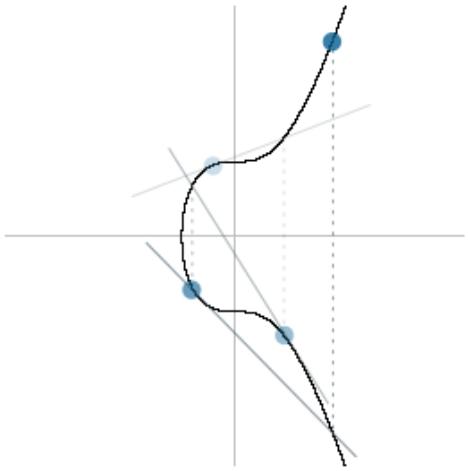
در مثالی که در بالا دیدیم با ضرب 2 در G به 2G رسیدیم.

برای بدست آوردن کلید عمومی ما ضرب می کنیم G رو با کلید خصوصی خودمون، مثال زیر رو ببینید:

```
private_key = ef235aacf90d9f4aadd8c92e4b2562e1d9eb97f0df9ba3b508258739cb013db2
private_key = 108165236279178312660610114131826512483935470542850824183737259708197206310322

public_key  = 108165236279178312660610114131826512483935470542850824183737259708197206310322 * G
```

با به عبارت دیگه با استفاده از چرخیدن در اطراف منحنی بیضوی به صورت های مختلف به شماره کلید خصوصی دست پیدا می کنیم.



You get the idea.

نقطه پایانی که بر روی منحنی بیضوی بدست می آید مختصاتی به شما می دهد و درواقع این مختصات همان کلید عمومی شما را تشکیل می دهد.

بنابراین اگه در نهایت این مختصات ما باشه، با ضرب G توسط کلید خصوصی ما ایجاد شده است:

```
x = 81591541406288143274758265124625798440200740391102527151086648448953253267255
y = 64573953342291915951744135406509773051817879333910826118626860448948679381492
```

بنابراین باید ما هردوی این ها رو به هگزادسیمال تبدیل کنیم، و اونها رو با هم ترکیب کنیم:

```
public_key (x) =
b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a8737


public_key (y) =
8ec38ff91d43e8c2092ebda601780485263da089465619e0358a5c1be7ac91f4


public_key (x,y) =
b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a87378ec38ff
91d43e8c2092ebda601780485263da089465619e0358a5c1be7ac91f4
```

این شکل اصلی کلید عمومی هستش، به این معنیه هستش که باید 04 رو در شروع اون قرار بدیم مثل این:

```
public_key =
04b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a87378ec38
ff91d43e8c2092ebda601780485263da089465619e0358a5c1be7ac91f4
```

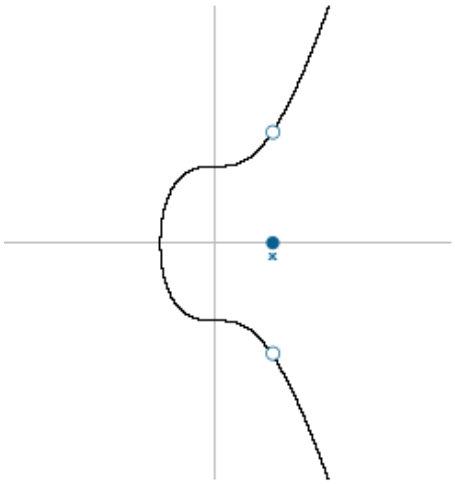
برای اینکه بفهمیم چرا به این صورت هستش، باید به بخش چگونگی فشرده کردن کلید های عمومی مراجعه کنید که به چه صورت این کار انجام می گیره. به هر حال این کلید عومی ایجاد شده ما می باشد.

فشرده سازی کلید عمومی

برای صرفه جویی از فضای استفاده شده، کلید های عمومی (این روزها) رو تنها با مختصاتی X مانند تشابه سازی می کنند.

این به این خاطره که منحنی بیضوی تشکیل شده از یک معادله می باشد (y2 = x3 + 7)، به این معنیه که اگه شما مختصات X رو دارید می تونید Y منتاظر رو بر طبق معادله بدست بیاورید.

با این حال، بدلیل اینکه Y^2 در این معادله داریم، Y ما می تونه عدد مثبت یا منفی باشه:



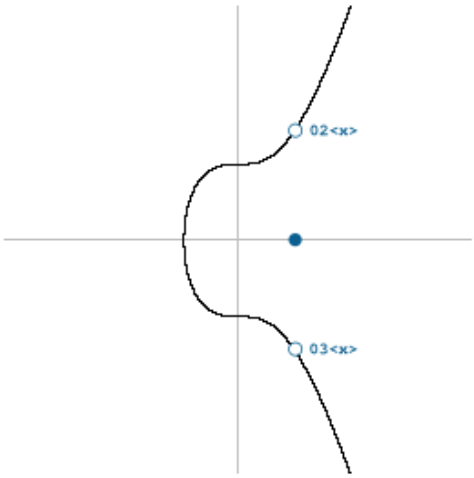
بنابراین تنها اطلاعات اضافی که شما نیاز دارید برای بدست آوردن مختصات دقیق Y باید ببینید مختصات Y در بالا یا پایین محور X باشد، و البته برگرفته از کارکرد منحنی بیضوی هم می باشد:

- اگه Y زوج باشه، بنابراین در بالای محور X هستش
- اگه Y فرد باشه، بنابراین در زیر محور X هستش

بنابراین بجای داشتن هر دوی اینها (X و Y) به عنوان کلید عمومی، شما می تونید فقط X رو ذخیره کنید، بدون اینکه در نظر بگیرید Y منفی هست یا مثبت !

در بیت کوین، قسمت زوج یا فرد بودن؛ را با پشفرضی در مختصات X نشان می دهند.

- زوج = 02
- فرد = 03



بنابراین در حالی که کلید عمومی اصلی با 04 شروع می شه، یک کلید عمومی که به صورت فشرده هست با 02 یا 03 شروع می شه:

```
public_key            =
04b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a87378ec38
ff91d43e8c2092ebda601780485263da089465619e0358a5c1be7ac91f4


public_key_compressed =
02b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a8737
```

همانطور که می بینیم به نظر می رسه که خیلی تلاش شده تا به متن کوتاهی دست پیدا بشه، زیرا بخاطر اینکه از کلید عمومی در تراکنش ها استفاده می شود، در نهایت در طول زمان منجر به صرفه جویی فضای زیادی در بلاکچین می شود.

چرا ما از ضرب کردن روی منحنی بیضوی برای بدست آوردن کلیدهای عمومی استفاده می کنیم ؟

از اونجایی که منحنی بیضوی دارای 2 ویژگی هستند که زمان ایجاد کلید خصوصی یا عمومی مفید واقع می شه.

1. ضرب منحنی بیضوی یک تابع trapdoor هست، به عبارت دیگه شما نمی تونید به عقب برگردید از این طریق (به عنوان مثال با تقسیم کلید عمومی) به منظور دستیابی به کلید خصوصی.

"یک تابع trapdoor یک تابعی می باشد که به صورت یک طرفه محاسبه می شود، و در محاسبه برعکس اون ینی از خروجی اون برگردی به ورودی بسیار کار مشکلی هست (معکوس آن)، و بدون اینکه در این بین اطلاعات خاصی انتقال پیدا کنه، اسم این تابع trapdoor هست.

2. با این وجود یک کلید عمومی به صورت ریاضی گونه به کلید خصوصی ارتباط برقرار می کنه، در نتیجه، ممکن هست که این اتصال (با استفاده از محاسبات ریاضی بیشتر) بدون داشتن کلید خصوصی اون رو آشکار کنه !

بنابراین اگه من کلید عمومی (یا آدرس) خودم رو به شما بدم، می تونم به شما اون رو بدم بدون اینکه به شما کلید خصوصی خودم رو نشون داده باشم.

این توانایی مخصوصا زمانی مورد احتیاج هست که من بخوام یک تراکنش بیت کوین ایجاد کنم که در این تراکنش شامل قرار دادن کلید عمومی من در داده های تراکنش باشه و درواقع اثبات این باشه که صاحب آن من هستم، و این امر به طوری انجام بگیره که بدون اینکه نیاز باشه من کلید خصوصی خودم رو در این داده ها بفرستم.

توجه داشته باشیم که کلید عمومی یک کلیدی هست که منحصر به فرد مربوط به کلید خصوصی مربوط به خودش هست، بنابراین زمانی که من می گم صاحب کلید عمومی من هستم، منظورم اینه که کلید خصوصی که مربوط به این کلید عمومی هست (که از روی کلید خصوصی ساخته شده) رو دارم و اون رو می دونم چیه.

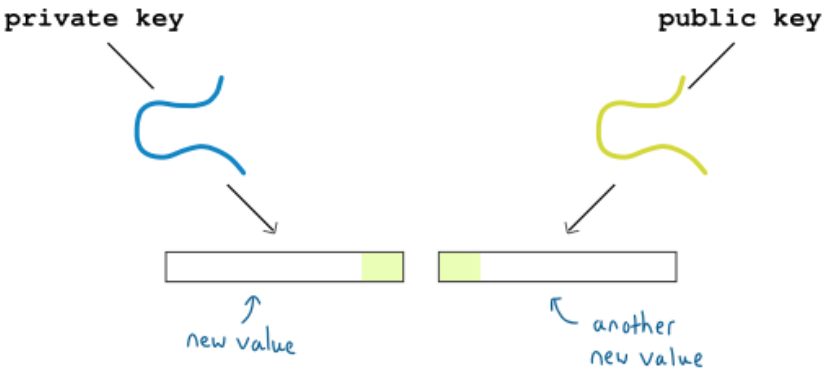
چطور می شه ثابت کرد که کلید عمومی متعلق به شماست ؟

این خودش یک موضوع کاملی رو در بر میگیره و شاید حتی 2 تا موضوع باشه، اما چون این یک موضوع به شکل مهمی به این مبحث مرتبط هست سعی می شه مفاهیم پایه ای اون رو یک توضیحی داده باشم.

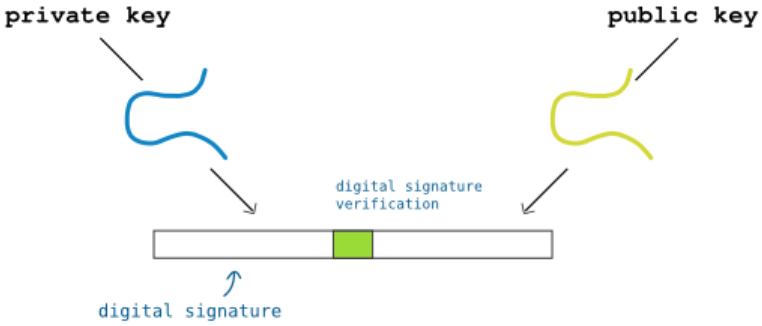
همانطور که ذکر شد، یک ارتباط ریاضی بین کلید عمومی و کلید خصوصی وجود دارد.

در نتیجه:

1. من می تونم کلید خصوصی خودم رو به منحنی بیضوی بدم و با محاسبات ریاضی که در آن انجام می گیره به یک مقدار(ارزش) جدیدی دست پیدا کنم.
2. من می تونم با قرار دادن کلید عمومی خودم در منحنی بیضوی های دیگه ای قرار بدم و از روی اون مقدار (ارزش) دیگه ای رو بدست بیارم.



در حال حاضر این مقادیر کمی که مشاهده می کنید، همپوشانی مقادیر جدیدی هست که بوجود آمده اند.



The new value I can create from my private key is called a *digital signature*

و...

این همپوشانی ثابت می کنه که رابطه ریاضی ای بین کلید عمومی و کلید خصوصی وجود داره.

و از اونجایی که کسی نمی تونه این امضای دیجیتال رو بدون داشتن کلید خصوصی مرتبط با اون ایجاد کنه، همین امضای دیجیتال بتنهایی ثابت کننده این موضوع هست که کلید عمومی متعلق به من هستش.

نتیجه.

همه این بالا پایین شدن ها زیر سر این منحنی بیضویه !!

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

شاد زی.

لئوناردو داوینچی: "هیچ دانشی را نمی توان واقعی دانست مگر این که به صورت ریاضی نوشته شود".