امضاء دیجیتال (امضاء کردن و تایید کردن)

(برگردانده رضا تجری)

امضاء کردن

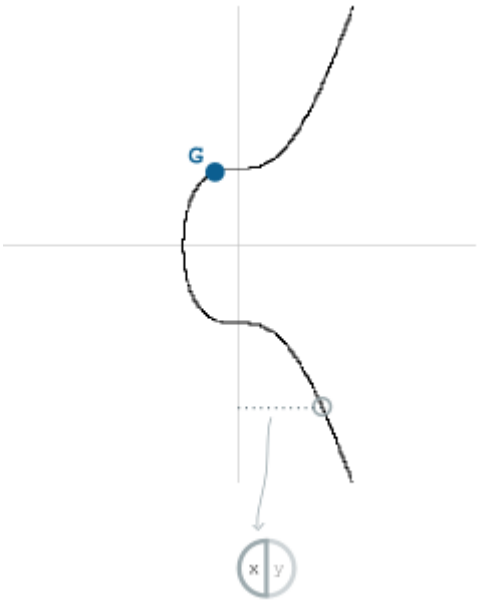
یک امضاء دیجیتال حاوی 2 بخش هست:

1. یک بخش تصادفی
2. یک بخش امضاء (کلید خصوصی + داده های تراکنش که امضاء دیجیتال رو برای اون ایجاد کردیم).

1. بخش تصادفی

این بخش شروعش با تولید یک عدد تصادفی انجام می گیره. سپس این قسمت رو ضرب در منحنی بیضوی می کنیم برای تولید نقطه روی منحنی بیضوی (شبیه همون کاری که برای ایجاد کلید عمومی انجام می گرفت):

قسمت شماره تصادفی که ما داریم همان نقطه ای هست که روی منحنی بیضوی ما وجود دارد. اما ما فقط مختصات x رو از اون می گیریم:



ما اینو "r" می نامیم موقتا.

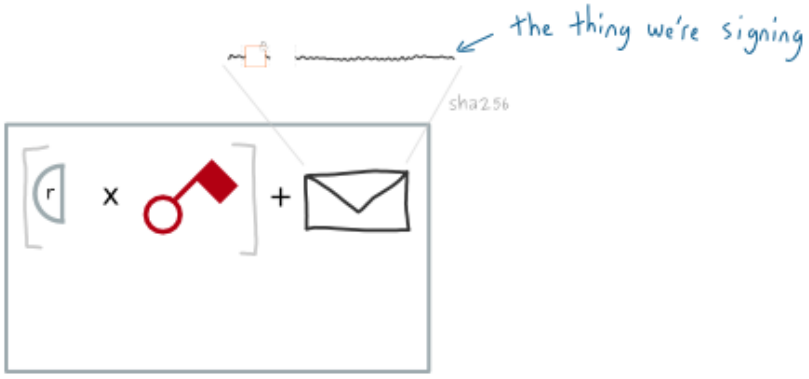
این اساسا شبیه ایجاد کلید خصوصی و کلید عمومی هست، اما در اینجا ما برای اضافه کردن یک المان تصادفی برای امضاء دیجیتال خودمون انجام می دیم.

خب حالا ما نصف امضاء دیجیتال خودمون رو آماده کردیم، اما ما هنوز از کلید خصوصی خودمون استفاده نکردیم، اینجاست که نصف دیگه ساخت امضاء دیجیتال رو شامل می شه...

2. بخش امضاء

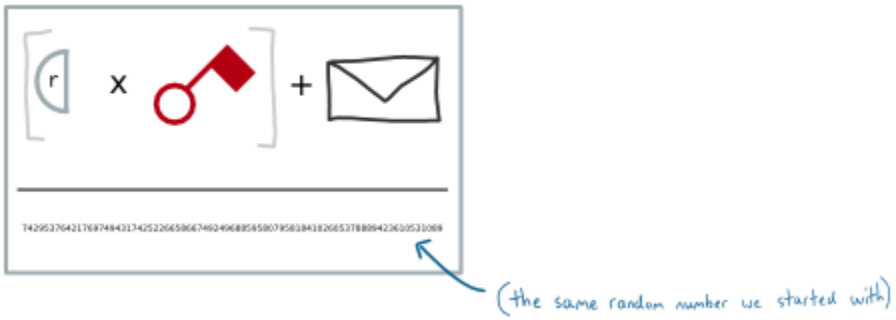
اول ما کلید خصوصی خودمون رو با r (همون مختصات x که نقطه تصادفی روی منحنی پیدا کرده بودیم) ضرب می کنیم.

مرحله بعد شامل مواردی می شه که ما می خواهیم امضاء کنیم. این قسمت رو پیام می نامیم در بیت کوین. پیام هش کل داخل داده های یک تراکنش هست که شامل خروجی ای می باشد که ما می خواهیم قفل اون رو باز کنیم.

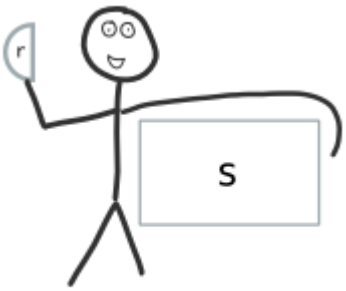


Including transaction hash ties the signature to one transaction (so it can't be used within a different transaction).

سرانجام برای حالت مناسبی رو ایجاد کنیم، همه اینها رو تقسیم بر عدد تصادفی می کنیم که اول با اون شروع کرده بودیم:



و خب در این قسمت ما به قسمت مهم و حیاتی "امضاء" از بخش امضاء دیجیتال خود رسیده ایم، که این رو موقتا S می نامیم.



Mr. D Signature.

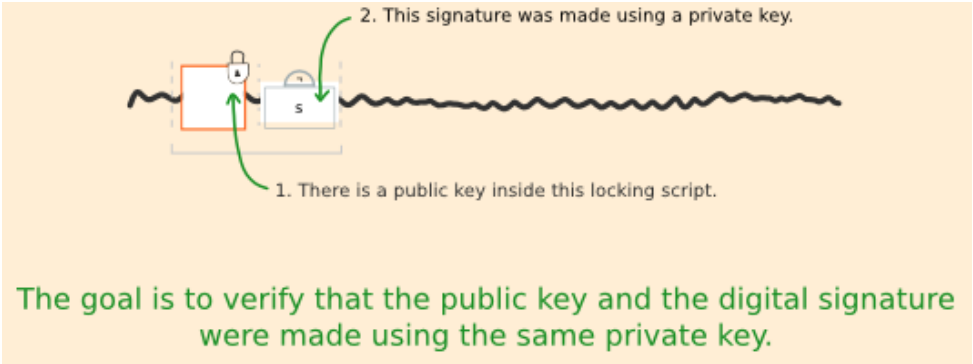
خب اینجاش کمی سرگرم کننده هستش...

اگه کسی از ما بپرسه که مدرکی که ثابت کنه کلید خصوصی که دارید مربوط به کلید عمومی که نشون میدید، یا بعبارتی ثابت کنید که شما کلید خصوصی مرتبط با کلید عمومی که ادعا می کنید رو دارید، می تونیم به عنوان مدرک این موضوع امضاء دیجیتالی خودمون (R & S) رو به اونها بدیم.

اما چطوری یکی دیگه می تونه این موضوع رو اثبات کنه ؟

تایید کردن

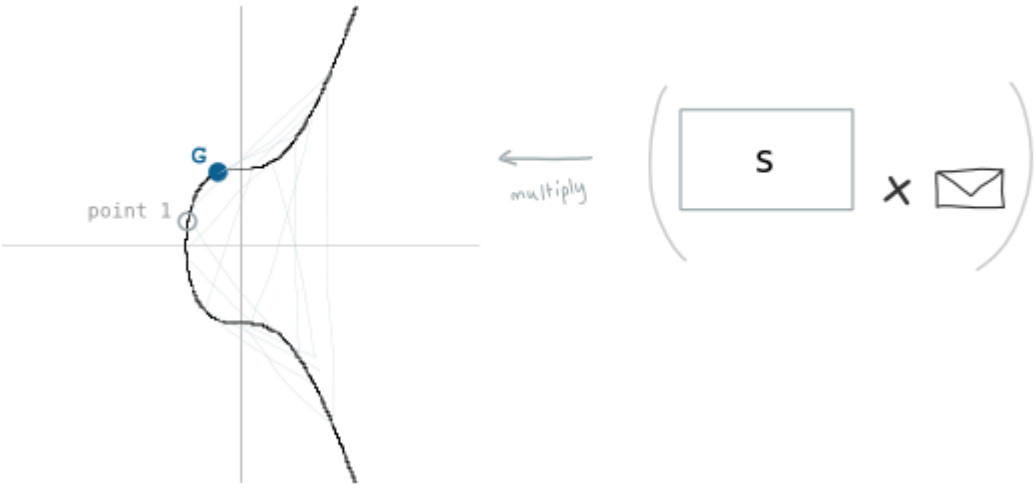
در بیت کوین، کل این امضاء می ره برای "باز کردن اسکریپت" که بخشی از تراکنش ها است. کلید خصوصی ما برای ایجاد امضاء استفاده می شود که ارتباط برقرار می کنه با آدرس که به آن قفل خروجی وصل شده است.



برای تایید امضاء دیجیتالی که از روی یک کلید خصوصی درست ساخته شده، شخصی که این امضاء دیجیتالی رو داده نیاز هست که از هر دو بخش آن استفاده کنه برای ایجاد 2 نقطه جدید بر روی منحنی بیضوی:

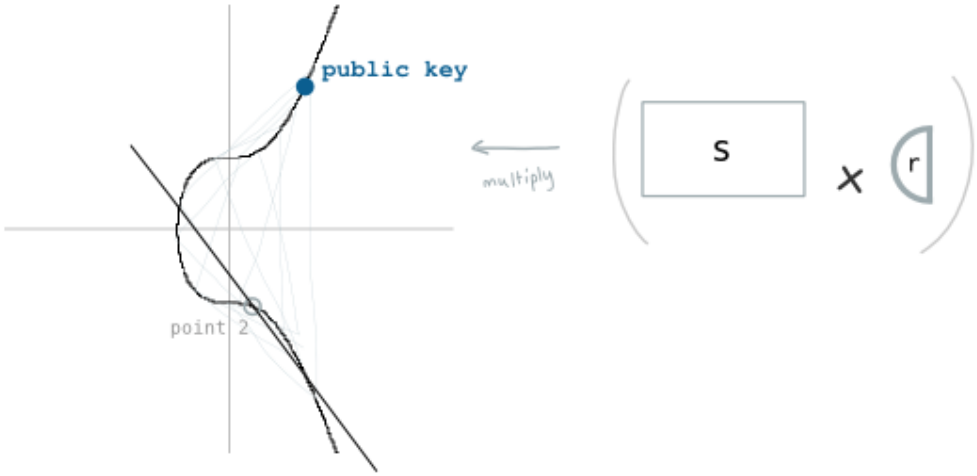
نقطه 1

S رو با پیام ضرب کنید. اولین نقطه که تنها توسط منحنی بیضوی ایجاد شده، ضرب نقطه توسط این مقدار می باشد:



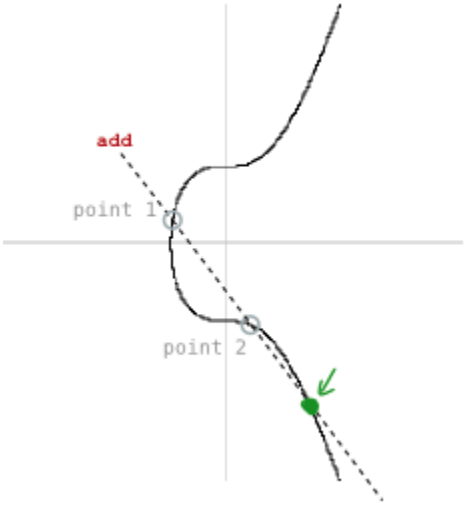
نقطه 2

S رو با r ضرب کنید. نقطه دوم تنها کلید عمومی ضرب شده توسط این مقدار هست:

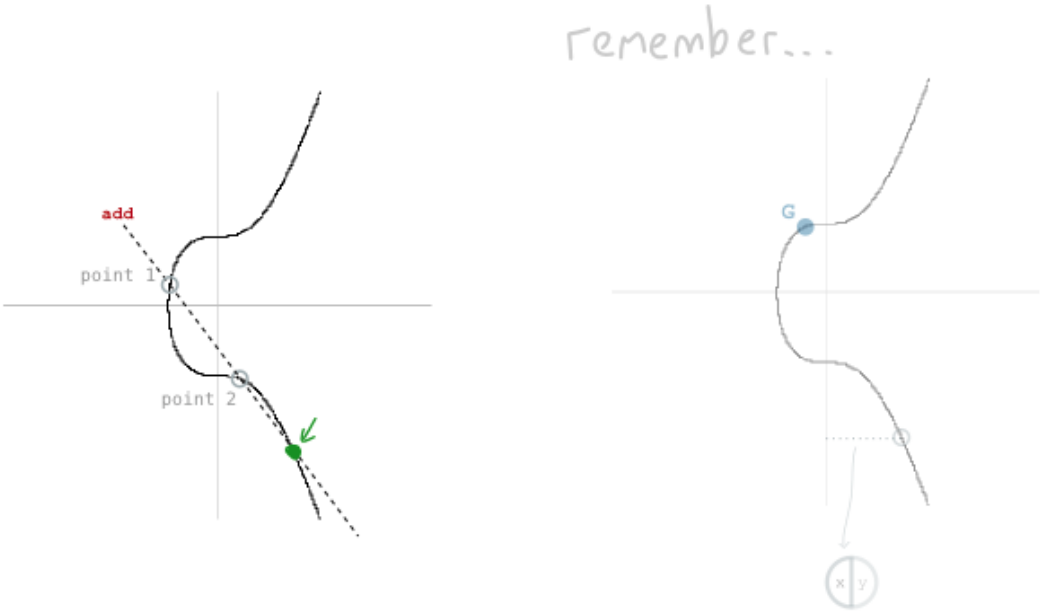


در انتها...

حالا اگه بیایم این 2 نقطه رو با هم دیگه جمع کنیم، یک نقطه سوم رو روی منحنی می تونیم بدست بیاریم:



و اگه مختصات x این نقطه سوم که بدست آوردیم شبیه مختصات نقطه x ای که در حالت تصادفی، (ینی زمانی که r رو داشتیم می ساختیم) بدست آوردیم باشه، این موضوع ثابت می کنه که امضاء دیجیتالی که داریم ایجاد شده بر اساس کلید خصوصی متصل به کلید عمومی ما می باشد.



یک ویدیو عالی به عنوان منابع که معرفی ای از قسمت های محاسباتی و تایید کردن امضاء دیجیتال رو آورده در اینجا قرار داده می شه. Bitcoin 101 - The Magic of Signing & Verifying

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

شاد زی..

اینم آخرین قسمت./