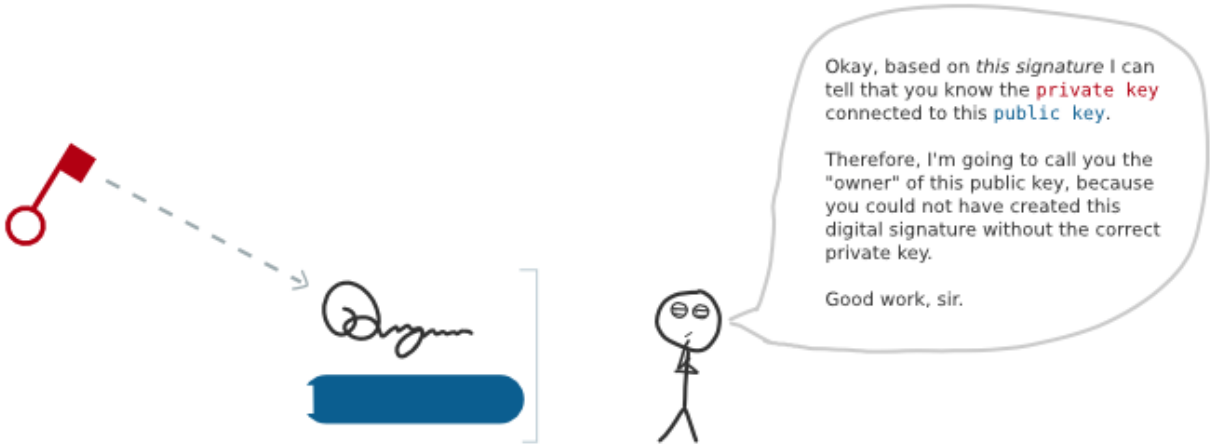
امضاء دیجیتال

(برگردانده رضا تجری)

یک امضاء دیجیتال چیست ؟

یک امضای دیجیتال در واقع نشان دهنده این هست که شما یک کلید خصوصی مرتبط به کلید عمومی مورد نظر خودتون رو دارید، و این کار در حالتی اتفاق میوفته که شما اطلاعاتی از کلید خصوصی خودتون رو نشون نمیدید.



بنابراین اگه کسی از شما پرسید آیا کلید خصوصی مرتبط با کلید عمومی (یا آدرس) خودتون رو دارید، می توانید با امضاء دیجیتال خودتون این موضوع رو اثبات کنید بدون اینکه کلید خصوصی خودتون رو به طرف مقابل نشان داده باشید.

شما فقط نیاز هست که کمی محاسبات ریاضی انجام بدید که ثابت کنید امضاء دیجیتالی خودتون مرتبط هست با کلید عمومی متناظر اون..

چرا از امضاء دیجیتالی در بیت کوین استفاده می کنیم ؟

زیرا زمانی که شما یک تراکنش می خواهید ایجاد کنید، باید قفل خروجی هایی که دارید رو باز کنید. برای این که بتونید نشون بدید که این خروجی ها برای شما هست و بتونید اون ها رو باز کنید باید بوسیله آدرس کلید خصوصی که دارید قفل خروجی ها رو باز کنید:

اما اگه شما کلید خصوصی خودتون رو در اطلاعاتی که در تراکنش هست قرار دهید، هر کسی می تونه در شبکه توانایی استفاده از اون رو داشته باشه:

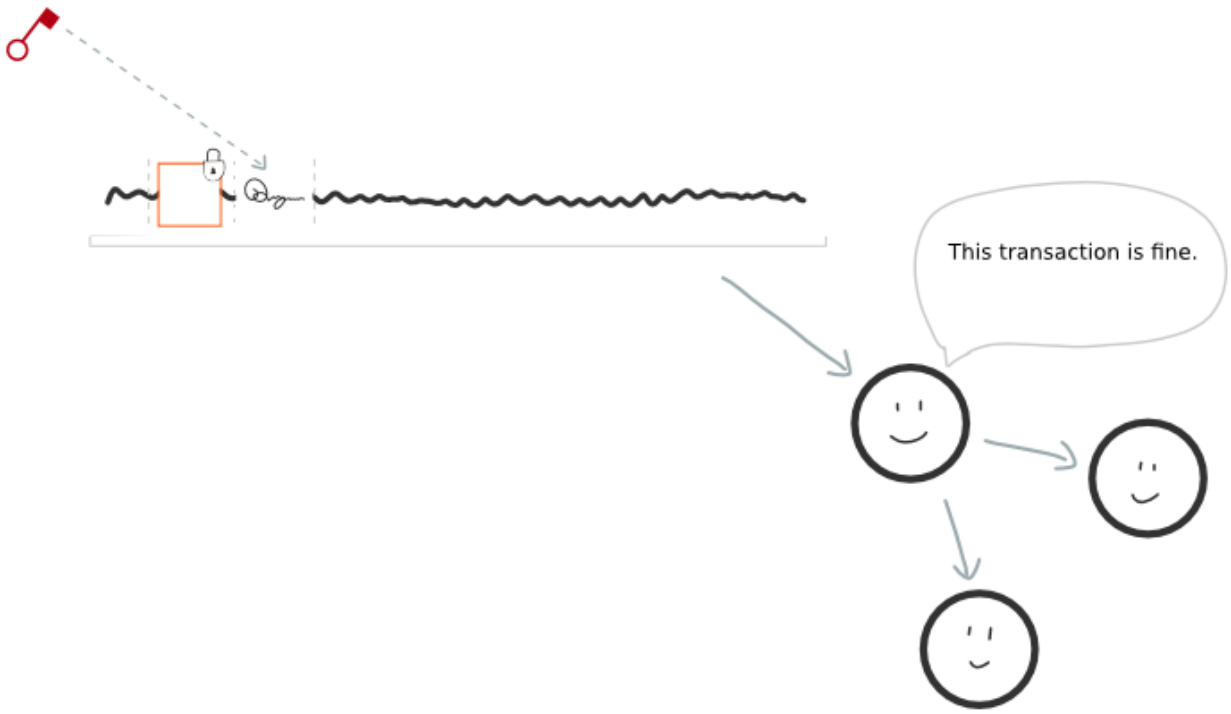
و اگه هر کسی کلید خصوصی شما رو بدست بیاره، می تونه بوسیله اون برای باز کردن و خرج کردن خروجی هایی که مرتبط به اون آدرس کلید خصوصی هست و قفل هستند انجام بده و مقادیر رو مصرف کنه.

خب پس چطوری می تونیم خروجی های قفل شده رو باز کنیم بدون اینکه کلید خصوصی خودمون رو نمایش بدیم ؟

امضاء دیجیتال رو وارد کنید.

امضاء دیجیتال می تواند برای باز کردن خروجی های قفل شده بکار رود، زیرا همین امضاء دیجیتال نشان دهنده این می باشد که ما کلید خصوصی مرتبط با آدرس خود را داریم.

نکته مهمی که در اینجا هست اینه که ما با داشتن امضاء دیجیتال، دیگه نیاز نیست که کلید خصوصی خودمون رو در شبکه انتقال بدیم.



به همین دلیله که ما از امضاء دیجیتال استفاده می کنیم بجای این که کلید خصوصی خودمون رو در معرض خطر قرار بدیم، و اون رو به همراه اطلاعات تراکنش به شبکه ارسال کنیم.

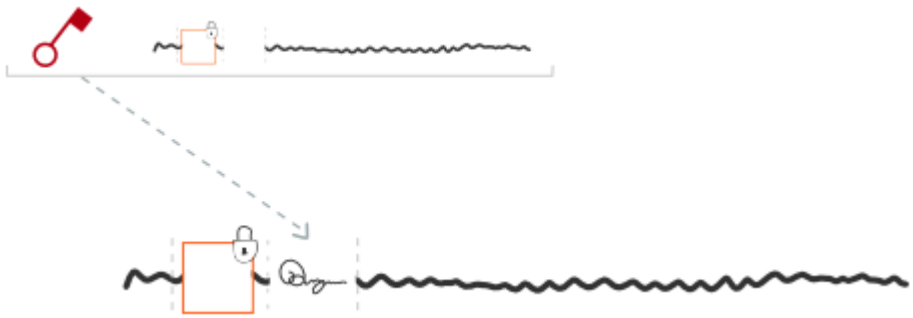
چطوری نزاریم شخص دیگه ای از امضاء دیجیتالی ما برای باز کردن بقیه خروجی های آدرس ما استفاده نکنه ؟

سوال خوبیه، اگه کلید خصوصی بتونه قفل های خروجی یک آدرس رو باز کنه، چرا کسی نتونه با داشتن امضاء دیجیتالی کاری شبیه همین کار کلید خصوصی رو انجام بده و خروجی ها رو باز کنه ؟

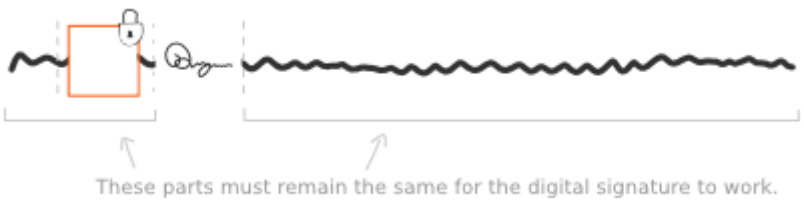
جواب: زیرا هر امضاء دیجیتالی در یک تراکنش، منحصرا مربوط به همون تراکنش می باشد.

- **بخوایم این رو یک تشابه سازی کنیم برای درک بیشتر می تونیم اون رو "مثل اثر انگشت از طریق fingerprint نمیشه ظاهر یک نفر رو دید ولی هر نفر fingerprint خصوصی خودشو داره."**

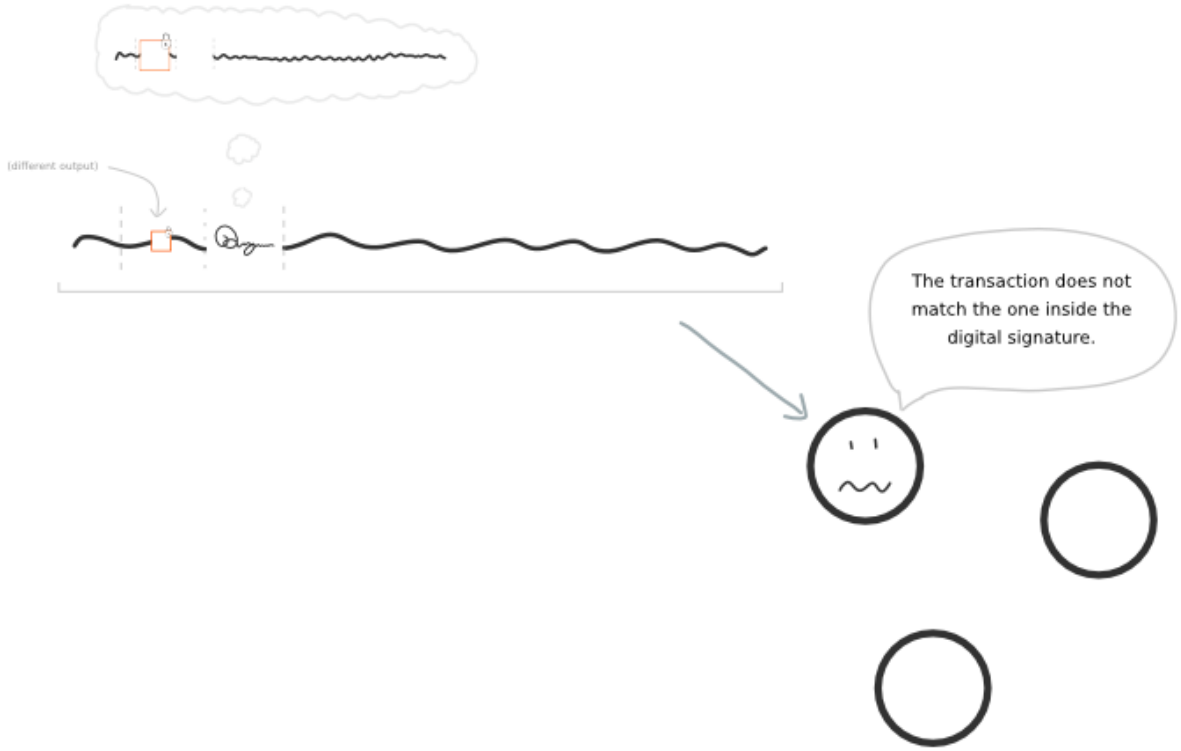
به عبارت دیگه، شما نمی تونید به تنهایی از کلید خصوصی برای ساختن امضاء دیجیتالی استفاده کنید، درواقع شما از کلید خصوصی خودتون و داده های اصلی که در تراکنش خودتون هستش استفاده می کنید:



بنابراین، هر امضاء دیجیتالی یک جورایی وصل (گره خورده – وابسته) به اون تراکنشی هستش که می خواهید اون رو انجام بدید:



خب بنابراین اگه کسی تلاش کنه با این امضاء بدست اومده برای تراکنش های دیگه انجام بده، منجر به درگیری با داده هایی که در داخل حافظه شبکه بیت کوین هستش، می شه و گره های شبکه بیت کوین اون رو قبول نخواهند کرد.



به عنوان یک نتیجه گیری می توان امضاء دیجیتال رو به عنوان نقش محافظت کننده در برابر هر کسی که بخواد از تراکنشی سوء استفاده کنه دانست.

امضاء دیجیتال چگونه کار می کند؟

و بازم ریاضیات.

1. شما ترکیب می کنید کلید خصوصی رو + داده های تراکنش، و برای ساختن امضاء دیجیتال از برخی محاسبات ریاضی استفاده می کنید.

2. پس از آن شما می تونید امضاء دیجیتال + داده ها تراکنش + کلید عمومی، رو بگیرید؛ و روی اونها عملایت ریاضی بیشتری رو انجام بدید، و در نتیجه تایید کنید که آیا برای امضاء دیجیتالی از یک کلید خصوصی معتبر و درست اینکار انجام گرفته است !

زیرا یادمونه که، **هدف امضاء دیجیتال این بود که ثابت کنه ما مالک کلید عمومی خودمون هستیم.**

میدونم این عملایت یکجورایی شبیه یک جادوگری دیده می شه، اما صادقانه بخوایم بررسی کنیم، ریاضیات دخیل در این موضوع هست.

و اگه شما علاقه دارید بدونید که چجوری کار می کنه...

- Digital Signatures (signing and verifying) (که این قسمت را در آینده برگردان خواهم کرد)

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

شاد زی..

علم داشتن نوعی قدرته، این یادمون باشه !