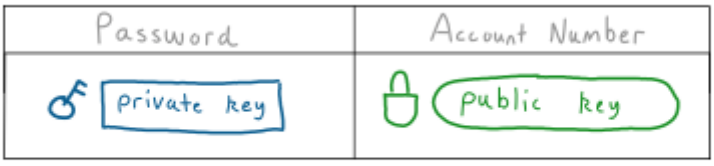
کلید ها و آدرس ها

(برگردانده رضا تجری)

یک کلید خصوصی، یک کلید عمومی، و یک آدرس چیست ؟

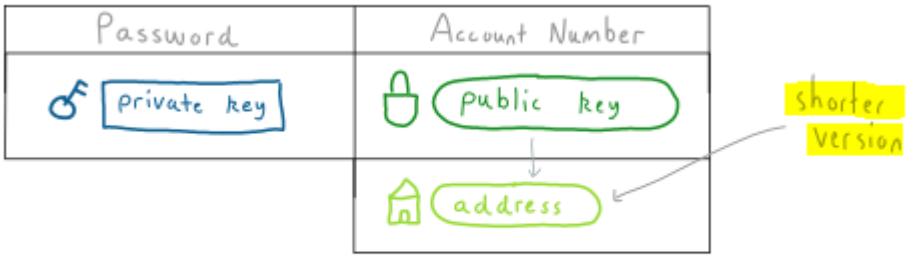
برای فرستادن و دریافت کردن پول به شکل بیت کوین شما نیاز به یک شماره حساب و رمز عبور دارید.

که البته در بیت کوین این 2 رو به نام های کلید عمومی و کلید خصوصی نامگذاری می کنند.



Here are your account details. Welcome to Bitcoin.

با این حال باید در نظر داشت که این شماره حساب زیاد مناسب نیست، (در ضمن از لحاظ تایپی هم سخته)، بنابراین برای اینکه بتوان از آن استفاده کرد نسخه کوچکتری از اون رو استفاده می کنیم، و اسم اون رو گذاشتن آدرس که درواقع همون آدرس ما می باشد.



You'll see how hideous the public key is in a moment.

و درواقع این نقش کلید خصوصی و کلید عمومی و آدرس رو بازی می کنه !!

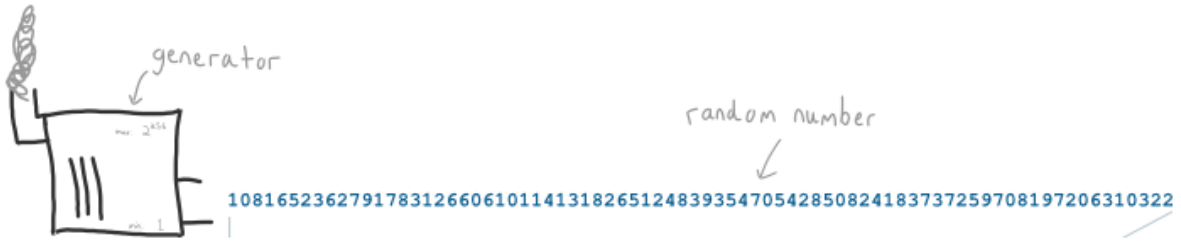
خب تا اینجا یک جمع بندی کنیم به طور خلاصه داریم:

- کلید عمومی شما، شماره حساب شماست.
- آدرس شما، شماره حساب شما محسوب میشه، اما نسخه کوتاه شده ای هست که مردم بتونن از اون استفاده کنند.
- و البته در اینجا در نظر داشته باشید که کلید خصوصی، رمز عبور شماست که مانع از این میشه که کسی دیگه نتونه از حساب شما بیت کوین به جایی ارسال کنه.

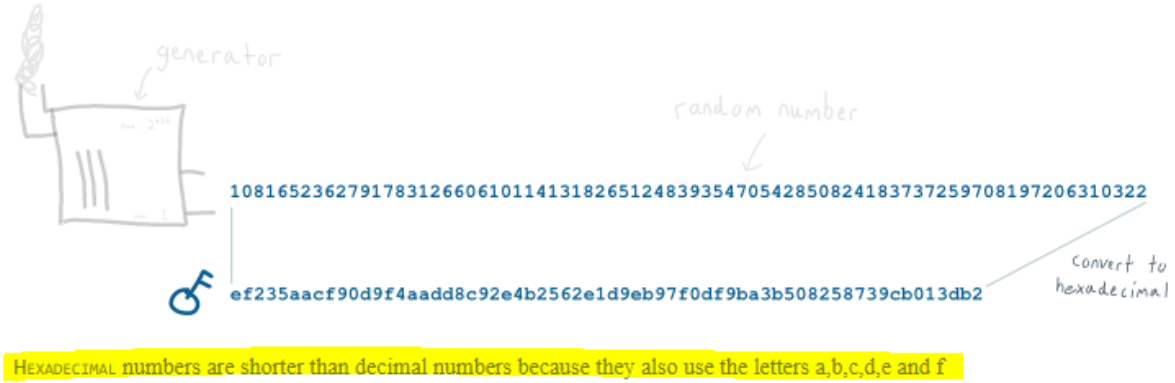
آدرس ها و کلید ها از چه جایی پدید می آیند ؟

کلید خصوصی

خب همه این جریانات از کلید خصوصی پدید می آیند، که تنها یک عملایت تصادفی ایجاد اعداد می باشد با هم شکل رو می بینیم تا بهتر متوجه مطلب بشیم:



اما چون این اعدا بسیار زیاد هست، کامپیوتر ها (و همینطور خود بیت کوین) علاقه به این دارن که از شکل کوتاه تری از این شماره ها استفاده کنند که اون حالت هگزادسیمال می باشد:



و ما همینطور که می بینید یک کلید خصوصی داریم که البته شامل اعداد بسیار طولانی هستش (منتها به شکل هگزادسیمال).

Private Key
ef235aacf90d9f4aadd8c92e4b2562e1d9eb97f0df9ba3b508258739cb013db2

- یک کلید خصوصی می تونه یک عدد بین 1 و 115792089237316195423570985008687907852837564279074904382605163 141518161494337 باشه.

کلید عمومی

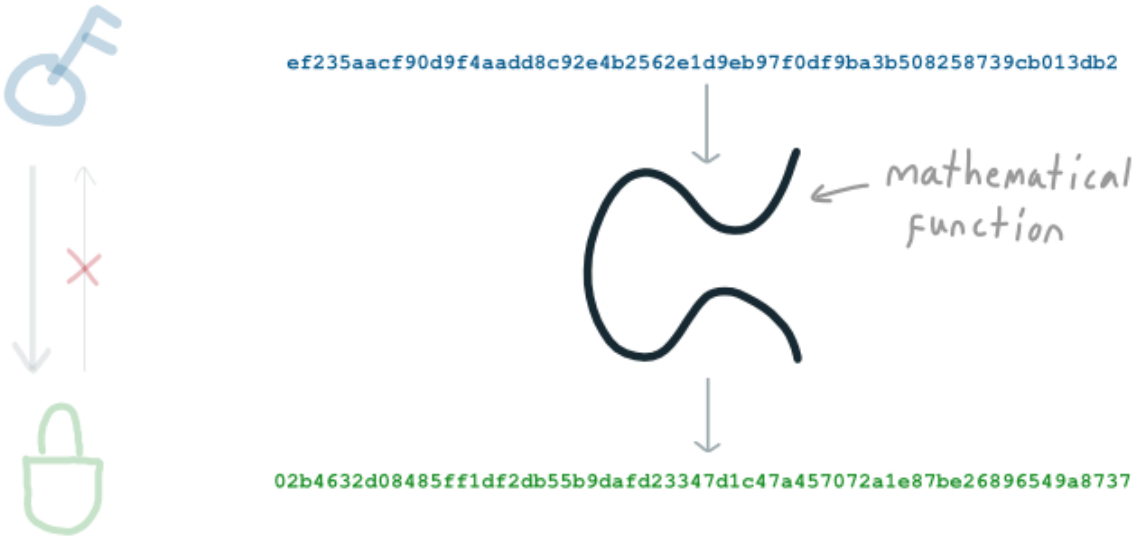
برای ایجاد کلید عمومی شما با استفاده از کلید خصوصی تون می تونید کلید عمومی رو ایجاد کنید !

اول از همه این رو بدونیم که کلید عمومی هستش که توسط بقیه مردم دیده می شه و می تونیم براشون ارسال کنیم تا مثلا بیت کوینی رو به اون حساب واریز کنند، بنابراین زمانی که ما استفاده می خواهیم کنیم از کلید خصوصی مون برای ایجاد کلید عمومی، ما نمیخوایم کلید خصوصی خودمون رو به کسی نشون بدیم زیرا کلید خصوصی باید نزد خودمون باشه، و کلید خصوصی هستش که از بیت کوین های ما حفاظت می کنه و اون مقادیر رو در بَر داره.

Even though the public key is made from the private key, we don't want anyone to be able to work backwards from it.

خوشبختانه می تونیم از یک نوع تابع خاص ریاضی برای رسیدن به این هدف دست پیدا کنیم.

ما تنها کلید خصوصی رو میدیم به اون تابع ریاضی، و در آخر تابع به ما یک کلید جدید میده بر اساس کلید خصوصی که داده شده که درواقع این کلید جدید همان کلید عمومی ما می باشد.



باید بدونیم که این تابع خاص ریاضی برای ما 2 مزیت داره:

1. این تابع ریاضی به ما یک کلید عمومی برمیگردونه که این کلید عمومی از اتصال یک کلید خصوصی بوجود آمده است، که درواقع برای زمانی که می خواهیم بیت کوین رو در قالب تراکنش برای کسی بفرستیم مفید واقع می شه.

It's like starting with a key and creating a padlock from it.

2. حتی اگه بخوایم این کلید عمومی ایجاد شده رو یکجوری به کلید خصوصی ربط بدیم، نمی تونیم یا چطور بگم خیلی سخته خیلی خیلی خیلی سخته که بشه از روی کلید عمومی به کلید خصوصی دست پیدا کرد، به همین دلیل هستش که از این تابع خاص ریاضی استفاده می کنیم، به طوری که این عملکرد یک حالت یک طرفه هستش، ینی از کلید خصوصی می شه به کلید عمومی رسید اما از کلید عمومی به کلید خصوصی خیر.

به لطف شماره های تصادفی ایجاد شده و این تابع خاص ما می تونیم بیت کوین های مورد نظر را فرستاده و همینطور دریافت کنیم، بدون اینکه کلید خصوصی خودمون رو به دست کسی داده باشیم یا کسی به کلید خصوصی ما از طریق کلید عمومی دست پیدا کنه..

Private Key	Public Key
ef235aacf90d9f4aadd8c92e4b2562e1d9eb97f0df9ba3b508258739cb013db2	02b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a8737

آدرس

خب ببینید تا الان ما به یک کلید عمومی رسیدیم که بازم شکل و شمایلش یک حالتی که شاید زیاد تمایل به تایپ اون داشته باشید، بنابراین میایم حالت عملی تری از اون رو معرفی می کنیم بنام آدرس.

Thank goodness for that!

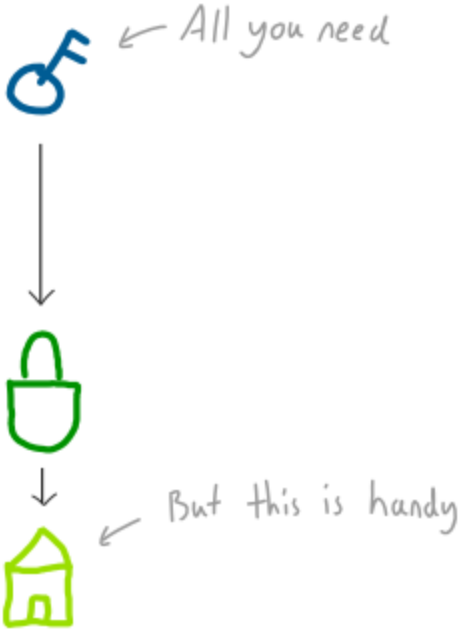
خب همانطور که در شکل بالا می بینید ما به نوعی کلید عمومی رو فشرده کردیم و به شکلی که اون رو آدرس می نامیم در آوردیم و از کاراکترهای مشابه ای مثل “l” or “o” ,“O” ,“0” استفاده نشده است. بنابراین ما تغییری رو تو ماهیت فهم کلید عمومی نبردیم و تنها اون رو بهبود بخشیدیم که به شکل مناسب تری دیده بشه و بتونیم راحت تر از اون استفاده کنیم، که این همون آدرس هستش.. یک نسخه کوتاه تر و ساده تر از کلید عمومی.

Private Key	Public Key
ef235aacf90d9f4aadd8c92e4b2562e1d9eb97f0df9ba3b508258739cb013db2	02b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a8737
	1EUXSxuUVy2PC5enGXR1a3yxbEjNWMHuem

خب یک نکته رو هم در اینجا بگم که با توجه به اینکه کلید به شکل فشرده ای در اومده و اون رو آدرس نامگذاری کردیم، باید بدونیم که در اینجا هم نمی تونیم از روی آدرس به کلید عمومی دست پیدا کنیم.

آیا ما باید همه 3 کلید ها رو بیاد داشته باشیم ؟

از اونجایی که کلید عمومی و همینطور آدرس بر گرفته از روی کلید خصوصی شماست، شما می تونید کلید خصوصی رو دور از کلید عمومی خود نگه دارید و در جایی امن ذخیره کنید.



Remember, your public key (and address) are worked out from your private key.

بنابراین اگه حتی در بدترین حالت ممکن باشه، اگه شما همیشه نیاز داشته باشید آدرس رو برای کسی بفرستید نیازی نیست کلید خصوصی رو برای کسی بفرستید و فقط کافیه آدرس خودتون رو که بر اساس کلید خصوصی بدست اومده رو ارسال کنید.

ببینید در حالت عادی بهتره که شما کلید خصوصی و آدرس خودتون رو در یک جایی نگهداری کنید، آدرس شما زمانی بکار میاد که شما می خواهید کسی براتون بیت کوین ارسال کنه بنابراین آدرس رو براش میفرستید تا توان فرستادن بیت کوین به حساب شما امکان پذیر بشه.

چه اتفاقی میوفته اگه کلید خصوصی رو از دست بدیم ؟

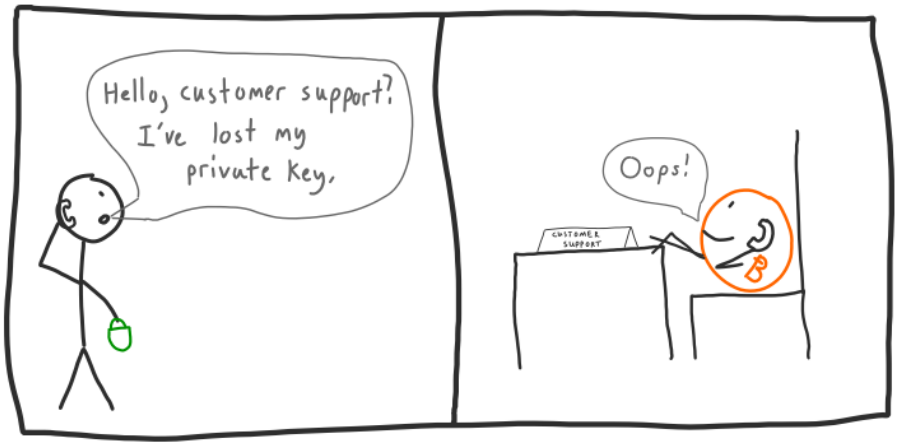
خب این می تونه بدترین اتفاق ممکن براتون باشه !

غیر ممکن (خیلی خیلی سخت) هستش که شما از روی کلید عمومی و یا آدرس خودتون به کلید خصوصی دست پیدا کنید، نتیجه اینه که اگه شما کلید خصوصی خودتون رو از دست بدید، کلید خصوصی خود رو از دست رفته بدونید !

باید توجه کرد که اگه شما کلید خصوصی مربوط به آدرس خودتون رو از دست بدید، مقادیری که در اون آدرس دارید رو از دست داده اید، و اگه به اصطلاح کلید خصوصی رو گم کنید، کل اون مقادیر که در آدرس خودتون داشتید از دست رفته !!

شاید بگید که این خیلی می تونه بد باشه، و خب بعله جواب اینه که همینطور هستش، کلید خصوصی اگه از دست بره ینی کل دارایی که در آدرس اون کلید خصوصی بوده از دست رفته.

و از سوی دیگه تنها کلیدی که به حساب شما می شه دسترسی داشت همین کلید خصوصی هستش، بنابراین کسی نمی تونه به جز شما مسئول اون باشه و توسط بک دور اون رو بدست بیاره، مگه اینکه خودتون مسائل امنیتی رو رعایت نکنید که کلید خصوصی رو از دست بدید، لطفا مراقب کلید خصوصی خود باشید !



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

شاد زی..