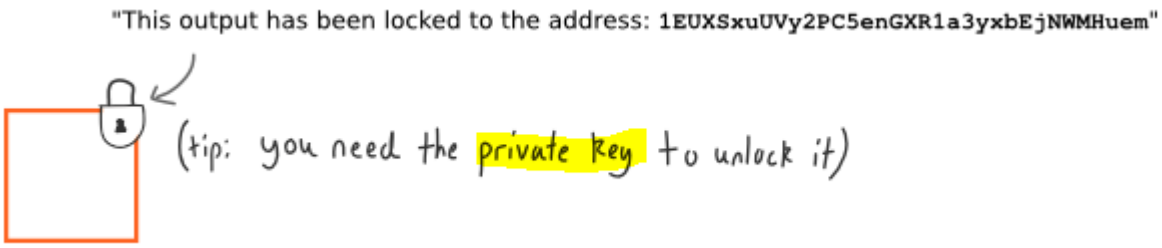
قفل های خروجی

(برگردانده رضا تجری)

یک قفل خروجی چیست ؟

قفل در خروجی ها به معنیه اینه که باید اول یک سری کارهای لازم انجام بشه تا بعد این قفل باز بشه تا قابلیت استفاده از خروجی رو به ما بده.

برای مثال عمومی ترین حالتی که می توان گفت در این مورد یک چیزی شبیه اینه:



این قفل ها باعث جلوگیری از استفاده آن ها می شه، ینی اینکه روی هر خروجی یک قفل زده شده، که تا زمانی که ما نخواهیم اون رو نمی شه خرج کرد و این قفل ها باعث می شن که تراکنش ها سرخود خرج نشن !

از چه جایی و متعلق به کجاست این قفل ها ؟

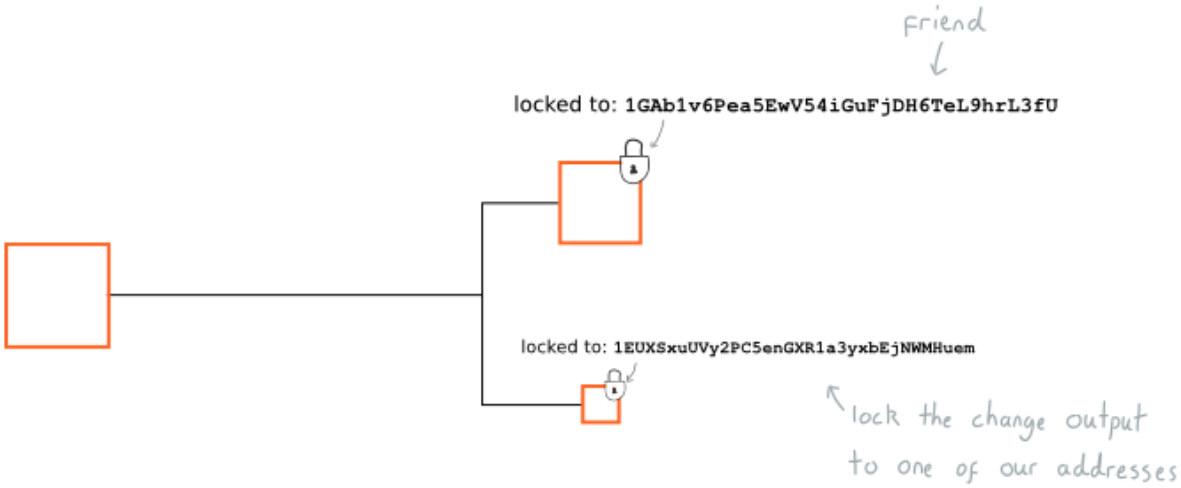
خب همونطور که می دونیم یک تراکنش فرآیندی هست بین خروجی های موجود و ایجاد نوع جدیدی از اونها:

A transaction.

در این حین که این خروجی ها ایجاد می شوند، به آنها همزمان قفل هم زده می شه:

Creating new outputs *and* giving each one a lock.

بنابراین بعد از اینکار ما یک خروجی جدید ایجاد کردیم که مثلا می خواهیم این رو برای دوستمون بفرستیم، وقتی اینکارو می خوایم کنیم بگونه ای انجام می گیره که تنها مالک (دوست ما) می تونه قفل این خروجی رو باز کنه و از اون استفاده کنه.

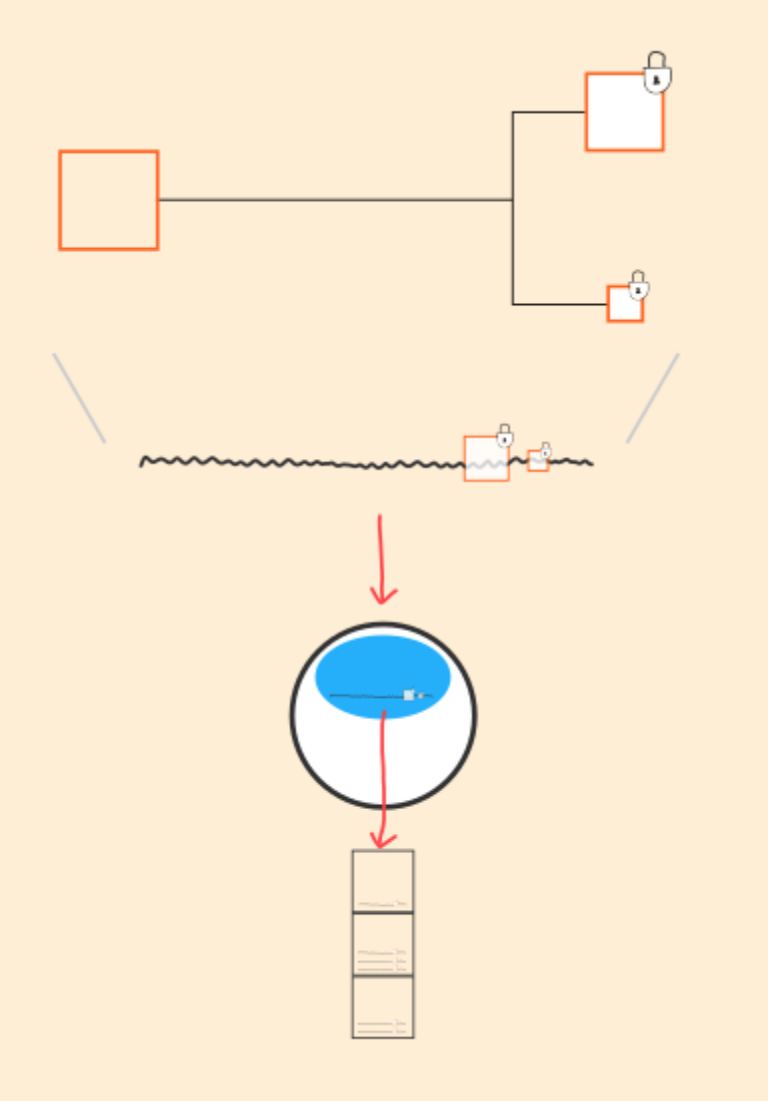


All of this is stored in the transaction data.

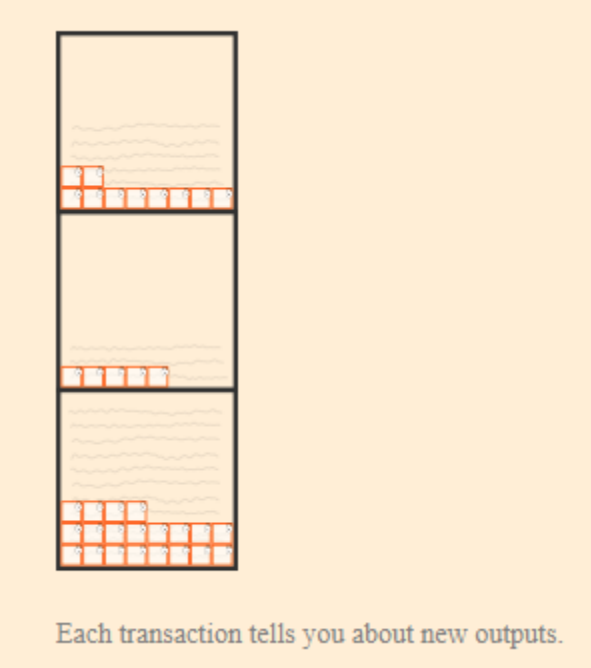
نتیجه چی میشه !؟ نتیجه اینه که وقتی ما این خروجی رو میفرستیم برای دوستمون و طوری قفل می زنیم که فقط اون استفاده کنه، بنابراین هیچ کس دیگه ای جز اون (دوست ما) که خروجی متعلق به خودشه نمی تونه قفل خروجی رو باز کنه چون تنها کلید دست دوست ماست که قابلیت باز کردن این خروجی رو داره.

همانطور که متوجه هستید هرگز بیت کوین ها رو در یک تراکنش ارسال نمی کنید.

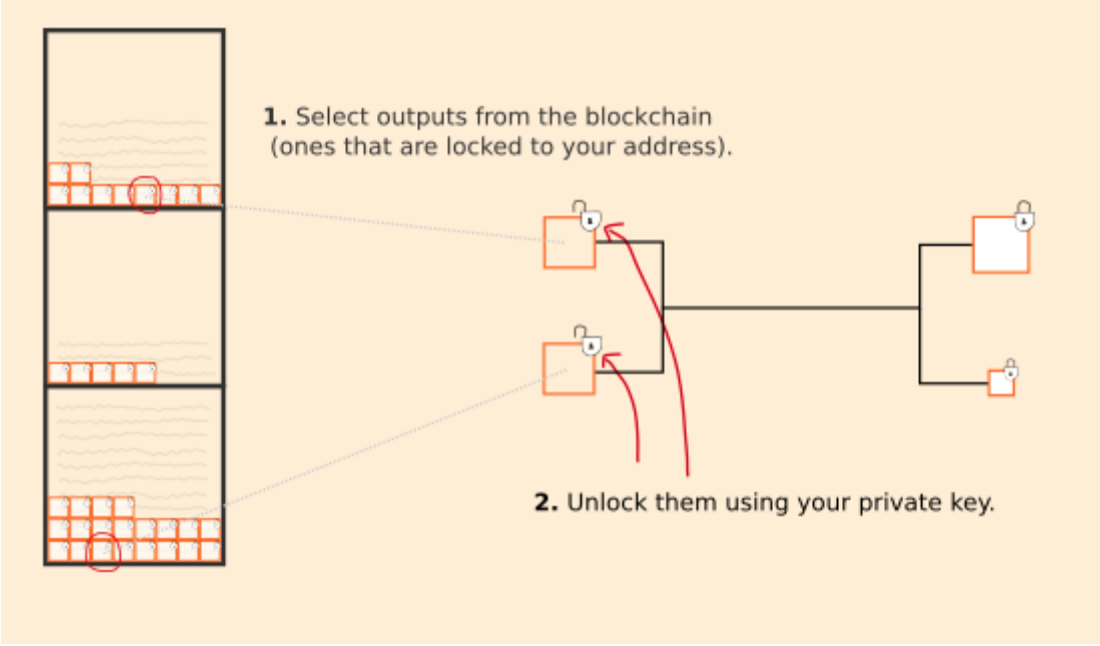
بجاش شما یک خروج جدید ایجاد می کنید (با قفل جدید) و این اطلاعات تراکنش رو به شبکه بیت کوین ارسال می کنید و منتظر این می مونید که استخراج گرها (ماینر ها) تراکنش شما رو به بلاکچین منتقل کنند.



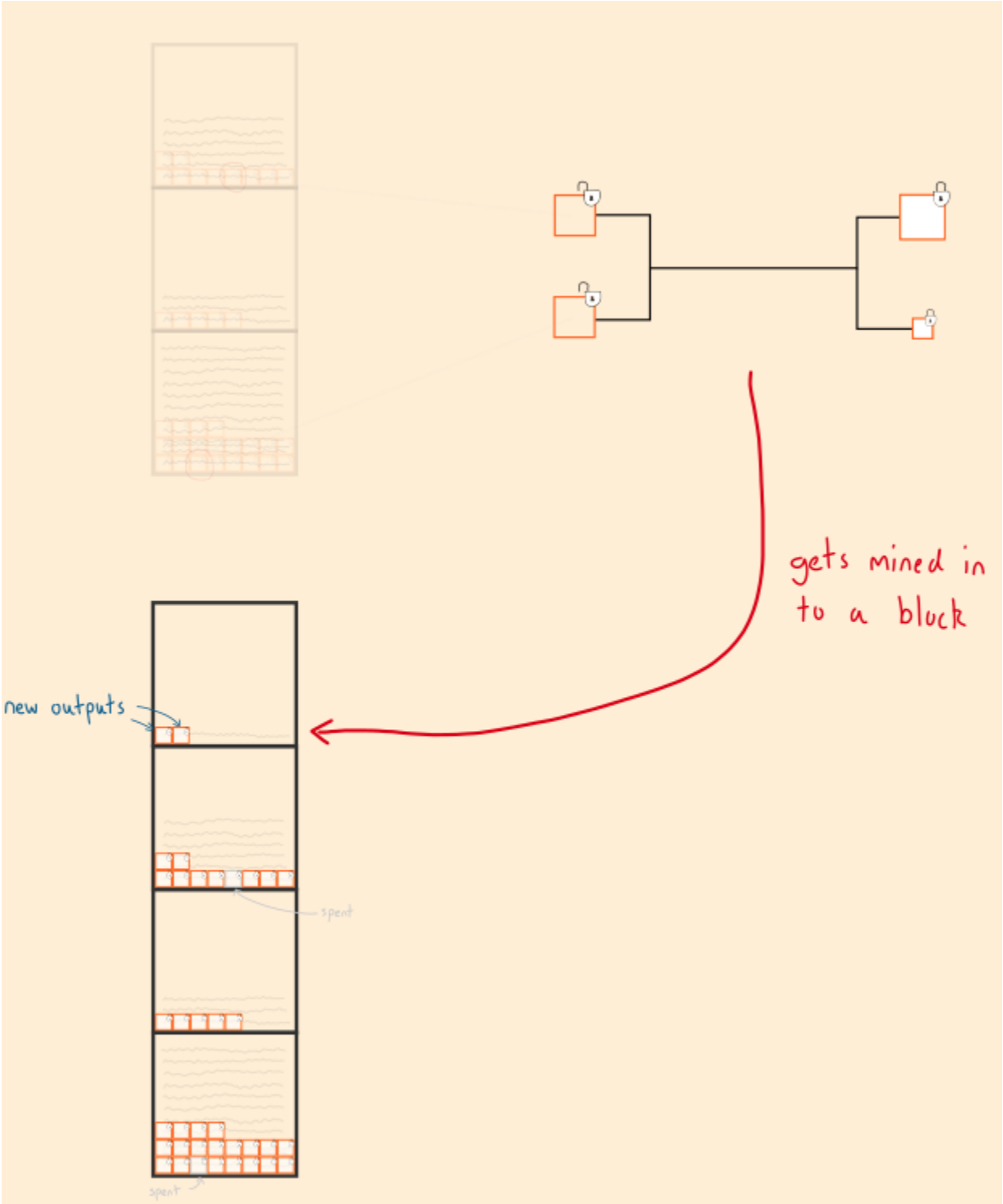
خب هرچند که بلاکچین یک سری فایل هستش، اما شما به هر حال به عنوان یک خروجی که به صورت عملی می توانید از آن استفاده کنید، می توانید از این تراکنش بهره ببرید.



و اگه زمانی شما نیاز داشته باشید که بیت کوین های خودتون رو برای کسی بفرستید به قفل بیت کوین هایی که در خروجی شما قرار دارند دسترسی دارید و قابلیت خرج آن را دارید.



و زمانی که شما این تراکنش رو خرج کردید و ماینرها اون رو به بلاک چین اضافه کردند دیگه این خروجی ها رو (نوعی ورودی) نمی توانید دوباره خرج کنید.



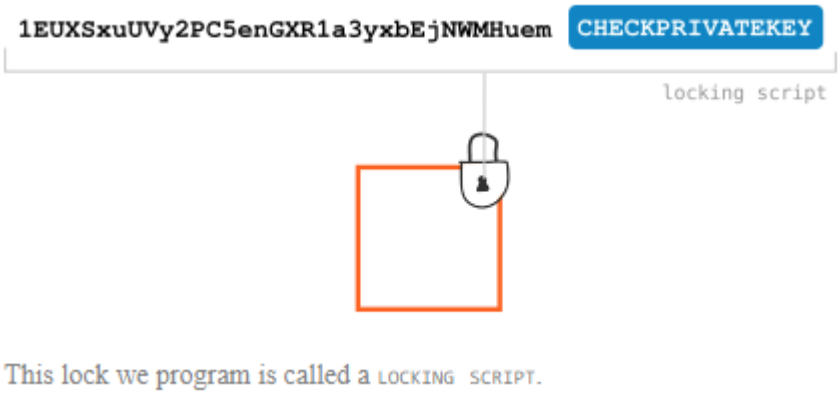
Each new block of transactions adds a fresh bunch of outputs in to the blockchain.

بنابراین بلاکچین یا همون زنجیره بلوک تمام خروجی ها رو در خودش زخیره می کنه و هر زمان که شما بخواهید می تونید از اونها استفاده کنید، و البته اینم میدونید که تا زمانی که شما دسترسی به قابلیت باز کردن خروجی ها رو داشته باشید یا به همون کلید خروجی ها رو در دست داشته باشید.

چگونه می توان یک قفل خروجی ایجاد کرد ؟

قفل خروجی در زبان برنامه نویسی که در قالب اسکریپت نوشته شده است.

این موضوع یکمی مشکله توضیح دادنش به صورت یک دیاگرام که به چه شکل عمل می کند، اما به هر حال یک چیزی شبیه به این شکل هست:



درواقع جالب ترین بخش این خروجی ها همان بررسی کردن پرایویت کی هستش، که در قالب یک تابع قرار داده شده که برای تنظیم نحوه قفل خروجی از آن استفاده می شود.

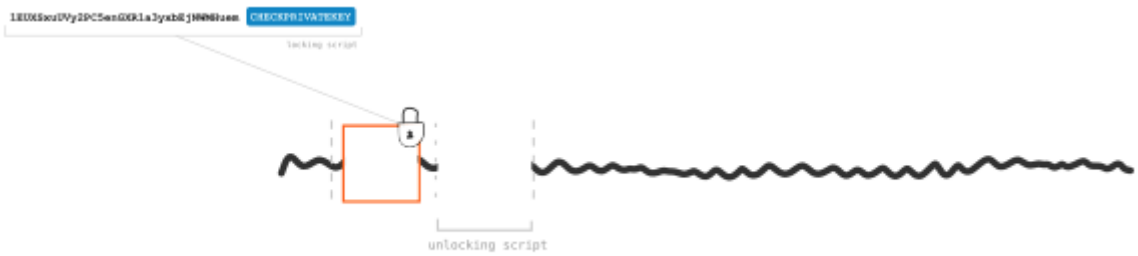
در مثال بالا برای نمونه ما خروجی را بطوری تنظیم کرده ایم که آدرس زیر را

1EUXSxuUVy2PC5enGXR1a3yxbEjNWMHuem با پرایویت کی مورد نظر این آدرس مقایسه کرده،

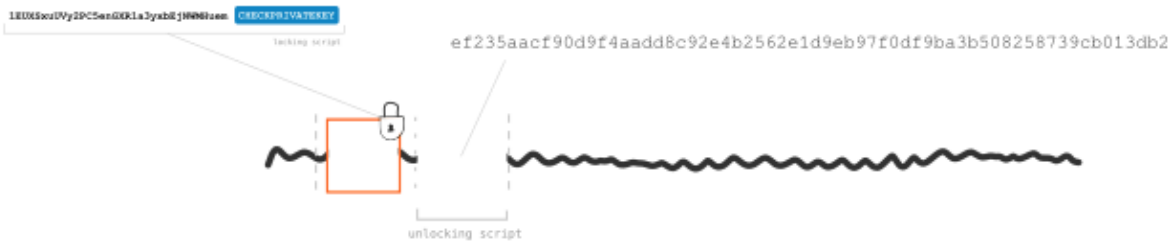
و پرایویت کی رو با این آدرس تطبیق بدیم، بعد از موفقیت این مرحله، می توان قفل رو باز کنیم و از تراکنش استفاده کنیم.

چگونه شما می تونید قفل خروجی رو باز کنید ؟

زمانی که شما جزئیات یک تراکنش رو ساختید، کنار آن اسکریپتی برای باز کردن قفل دارید "unlocking script" که برای استفاده از هر خروجی این اسکریپت رو به کار می‌گیرید.



بنابرانی برای باز کردن یک نمونه قفل اسکریپت (به عنوان مثال [address][CHECKPRIVATEKEY])، ما باید ثابت کنیم که آدرس که در پرانتز هم بود، رو داریم برای انجام این کار، و ما توسط کلید خصوصی که داریم می تونیم برای امضاء دیجیتالی از ان استفاده کنیم که جزئی از عملیات کار می باشد.



You put your digital signature as the “unlocking script”.

خب بعد از این زمانی که این داده های ارسالی رو یک نود در شبکه دریافت می کنه، میاد بررسی می کنه که اسکریپت های "locking" + "unlocking" با هم دیگه اجرا بشن و بررسی می کنند با آدرسی که داشتید

مطابقت داشته باشه، درواقع نگاه می کنند که قفل مرتبط باشه با آدرس و امضای دیجیتالی که ارسال شده است از طرف شما.

اگه همه چیز اوکی باشه نود (گره) تراکنش رو قبول می کنه و اون رو ارسال می کنه به نود های دیگه که هر کدام به عنوان نود در شبکه میان "locking" و "unlocking" رو بررسی می کنن و بعد اون تراکنش رو قبول می کنند.

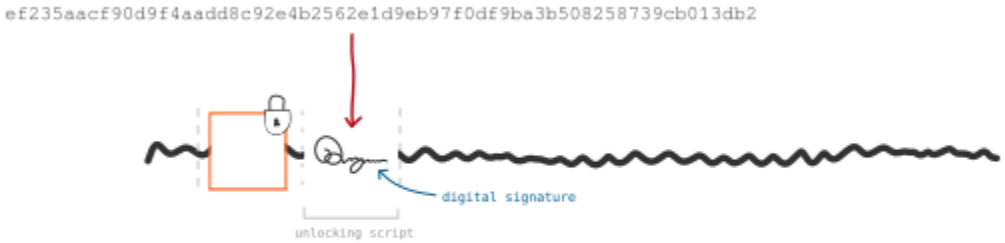
و اینجوریه که درواقع روند باز کردن یک قفل خروجی انجام میگیره.

چه چیزی می تونه ترسناک باشه ؟ پرایویت کی ای که همینجوری از دست بره !

دقت کنید به این موضوع عزیزان !

اعتراف: ما درواقع کلید خصوصی خودمون رو در اطلاعات دیتا تراکنش قرار نمی دهیم، این نکته رو اشتباه متوجه نشیم !

برای اینکه ما از پرایویت کی خود محافظت کنیم و اون رو در معرض خط قرار ندهیم، و همینطور داخل دیتایی ارسال نکنیم، تنها یک امضای دیجیتالی انجام میدیم، نه اینکه پرایویت کی رو برای کسی بفرستیم.



We use our private key to make a digital signature.

درواقع چیزی که از تابع هایی که ما استفاده می کنیم دروغی بود که به شما گفتم ☺ اما این موضوع ترسناک نیست، چون در واقعیت این موضووع مقایسه کردن وجود دارد و باید حتما یک پرایویت کی مخصوص آن آدرس باشه که با هم دیگه مقایسه بشه، که می شه مقایسه امضای دیجیتالی شما با مقایسه آدرس.. که این رو به اصطلاح CHECKSIG نام گذاری می کنند.

Still does the trick.

بنابراین یه دستت درد نکنه اساسی به امضای دیجیتال باید گفت که به لطف اون و البته تابع CHECKSIG، ما می تونیم خروجی هامون رو قفل بزنیم و اون ها رو خرج کنیم و همه این کارها بدون اینکه پرایویت کی خودمون رو در دست کسی دیگه قرار داده باشیم.

همیشه یادمون باشه پرایویت کی خیلی خیلی خیلی مهم هستش و باید بسیار مراقب اون باشیم زیرا هرکسی اون رو داشته باشه دسترسی به کیف پول شما داره !

یک فرآیند کامل و عالی !

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

به یادش: بسیار سفر باید تا پخته شود خامی

تمومه این قسمت !

شاد زی..