

# خروجی ها

## (برگردانده رضا تجری)

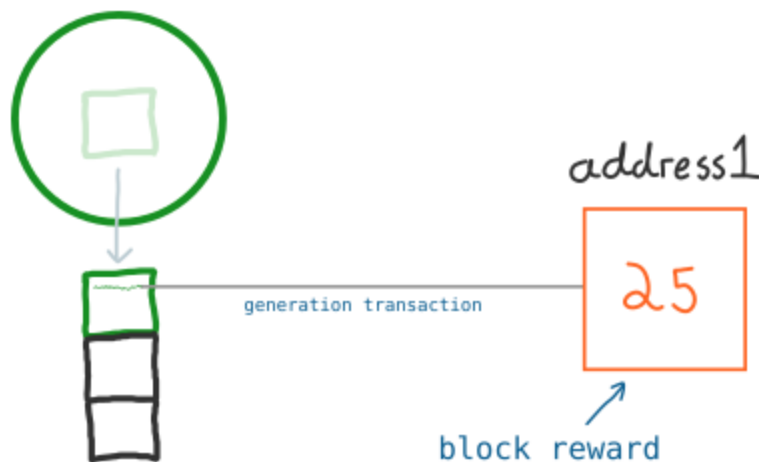
سیستم تراکنش های بیت کوی در بر گیرنده دسته های مقادیر بیت کوین که شامل فرستاده ها و رسیده ها هست ایجاد می شود که اینها را با نام خروجی ها نام گذاری می کنند.

برای اینکه متوجه بشیم به اندازه کافی که این عملیات به چه صورت انجام می گیره بهتره که چندین مثال بزنیم تا به این مسئله پی ببریم.

### تراکنش 1 – یک تراکنش ساده

می خواهیم این فرآیند را با استفاده از ایجاد شدن دسته ای از یک تراکنش جدید شروع کنیم...

شما یک استخراج کننده بیت کوین هستید، بر اساس کاری که انجام دادید موفق شده اید که یک بلوک از معاملات را حل کنید و دسته از بیت کوین ها که مقدار آن 25 عدد هست را بدست آورده اید.



باید توجه داشت که هر ماینر (استخراج کننده) آدرس خودش رو بالای هر بلوک قرار می دهد. با این تفاسیر اگه موفق به حل بلوک شوند مقدار جایزه بیت کوین بابت این زحمت کشیده شده، به آدرس مورد نظر ریخته

می شود.

بنابراین این اون چیزیه که از وضعیت فعلی ادرس بیت کوین استخراج کننده می بینیم:



به طور طبیعی و غریزی وقتی یک همچین مبلغی به حساب شما می شینه جشن میگیرید و با خودتون میگوید  
برم یک خرجی کنم بابت این زحمتی که کشیدم و مرشو بچشم، بنابراین با مقداری از اون تصمیم می گیرید  
برای خودتون خرج کنید، شایدم پولتون اضافه بیاد و هوس از دست دادنش به سرتون زد و ریختید تو سایت  
های پانزی و اسکم و اون رو ریختید تو جیب کلاه بردارها !!



بنابراین اولین چیزی که شما می خواهید انجام بدید اینطوره که به طور مثال 1 دونه از اون 25 بیت کوین که با  
سختی بدست آوردید رو خرج کنید، ینی 1 دونه از دسته ی 25 تایی خودتون می خواهید خارج کنید؛ این  
موضوع حساسیه، اما این کار به چه صورت انجام می گیره.



بجای اینکه ما 1 بیت کوین ارسال کنیم باید مجموع (کل) 25 بیت کوین که بدست آوردیم رو ارسال کنیم. اما برای اینکه مطمئن باشیم کل 25 بیت کوین رو نمی‌خواهیم؛ برای چیزی پرداخت کنیم که فقط 1 بیت کوین نیاز هست بنابراین ما این دسته رو تقسیم می‌کنیم به 2 مسیر مجزا، توجه کنید که اینجا همه واقعا:

1. جایی که می‌خواهیم 1 بیت کوین رو خرج کنیم
2. بازگشت به آدرس خودمان (یا جایی که مد نظر ماست)

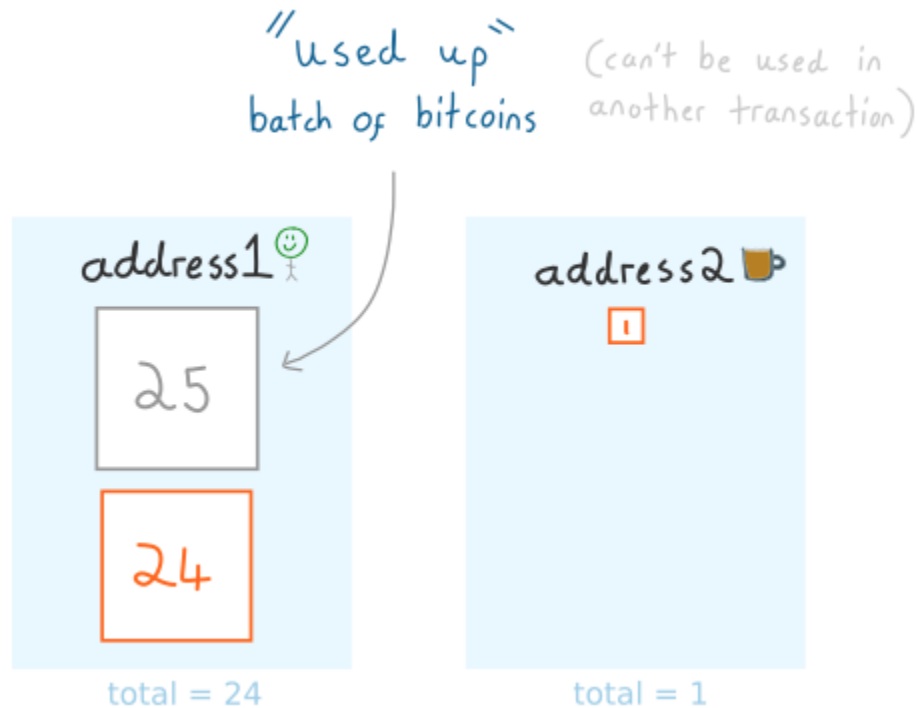


The newly created batches are called outputs.

درسته اینجا در ظاهر و لحظه ابتدایی یک لقمه رو دور سر خودمون چرخوندیم ولی در نهایت نتیجه یکسان هست، ینی هدف ما این بوده که 1 بیت کوین از 25 بیت کوین رو خرج کنیم، در ساختار تراکنش‌های خروجی بیت کوین به این شکل اون 1 بیت کوین خرج می‌شه، ینی 25 تا میره یکی ازش کم میشه باقیش برمیگرده به جایی که باید برگرده! ها ها

- جالبه بدونیم که دلیل اینکه به این صورت این تراکنش‌ها انجام می‌گیره، راه ساده و امنیت داشتن اون از دیدگاه برنامه‌نویسی می‌باشد.

به هر حال! در شکل زیر می بینیم که آدرس های بیت کوین بعد از این فرآیند به چه شکل می شوند:



در نتیجه فروشگاه یا اون جایی که ما 1 بیت کوین رو خرج کردیم، یک دسته جدید 1 بیت کوینی داره، خودمونم که یک دسته ایجاد کردیم که 24 بیت کوین توشه و این 2 از دسته اول (اصلی) که حاوی 25 بیت کوین بود ایجاد شدند.

بنابراین در ظاهر درسته که ما فقط می بینیم 1 بیت کوین را از حساب خود خارج کرده ایم، اما الان با اتفاقاتی که برای این فرآیند انجام می گیرد هم آشنا شده ایم.

## خلاصه:

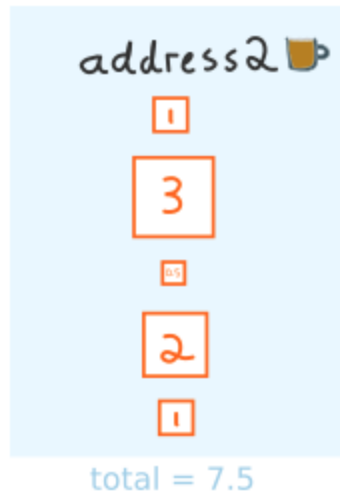
چگونگی طراحی انجام فرآیند تراکنش در بیت کوین:

1. داشتن یک خروجی که به صورت دسته در حساب ما می باشد
2. ایجاد کردن دسته جدید (با توجه به مقدار ارسالی برای حساب هدف)، از حساب خود
3. فرستادن این دسته جدید به آدرسی که مد نظر ما می باشد

## تراکنش 2 – استفاده از خروجی به عنوان ورودی

خیله خب از این به بعد بجای استفاده از کله دسته های از مقادیر از کلمه خروجی ها استفاده می کنیم.

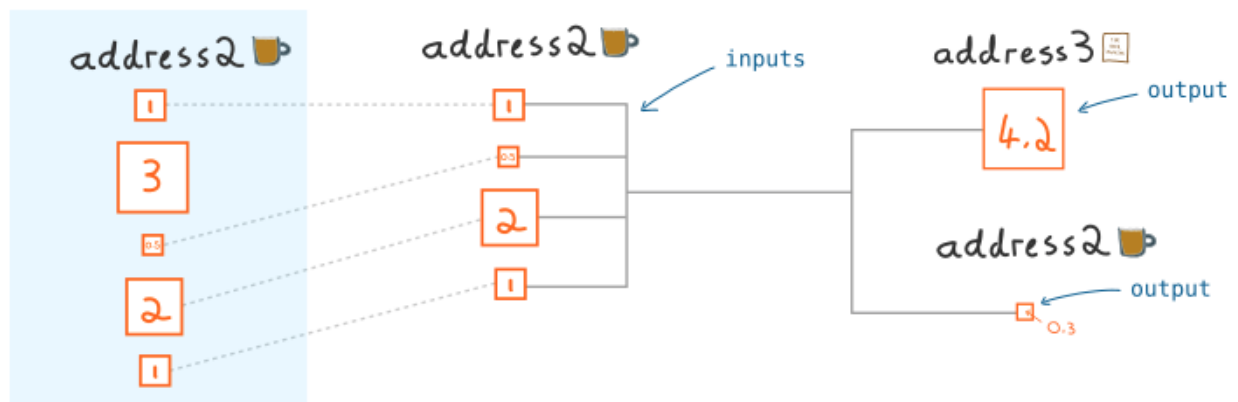
بعد از اینکه مغازه یا هر مکان دیگه ای که با بیت کوین اجناس خودش رو فروخت به همین طریق بیت کوین ها به حسابش می شینن و کسب و کار خودش رو راه می ندازه.



اما همانطور که می دونیم، فروشگاه نمی تونه مثل یک درخت رشد کنه، بنابراین باید تجهیزات خودش رو اضافه کنه و قدیمی ها رو بده و جدید بگیره و یک پیشرفتی در خودش بده که توسعه بیشتر پیدا کنه.



یکی میاد و این آگهی رو میبینه، و همینطور مشاهده می کنه که با بیت کوین به قیمت 4.2 بیت کوین به فروش گذاشته شده، بنابراین تصمیم به خرید اون گرفته می شه..

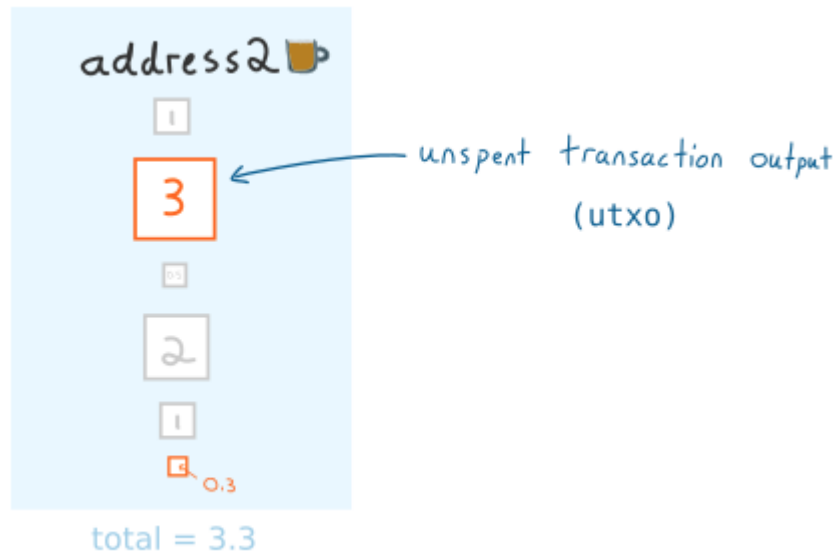


Constructing the transaction for the beer machine.

اما در این شکل حالت هایی رو می بینید که در اون چند نکته وجود داره که البته توضیح اون سخت نیست:

1. فروشگاه ما برای خروجی (دسته) خود تنها یک خروجی نداره که اون یک خروجی کل 4.2 مقدار بیت کوین رو پوشش بده، بنابراین باید یک جوری این دسته ها با هم جمع و جور بشن که در نهایت به 4.2 برسه که به خروجی مورد نظر دست پیدا کنه.
2. زمانی که ما یک تراکنش را می خواهیم انجام بدهیم، خروجی هایی که برای معامله انجام می گیرند تبدیل به ورودی هایی می شوند که می خواهیم از آنها برای ارسال استفاده کنیم برای آدرس مورد نظر. نکته: برای همین زمانی که شما از یک خروجی استفاده می کنید در یک تراکنش، این خروجی را به طور موقت بنام ورودی در نظر می گیرید !!
3. با توجه به اینکه مجموع کل 4.5 هست بنابراین باید خروجی ها با شند که یکی 4.2 و ما بقیش 0.3 ایجاد شوند.

بعد از انجام این فرآیند شکل تراکنش بیت کوین و عملیات معامله در حساب به شکل زیر می شود:



به این نکته هم توجه کنیم که خروجی هایی که به عنوان ورودی از آنها استفاده کردیم و ینی اونها رو خرج کردیم؛ دیگه نمی شه از اونها دوباره استفاده کرد و خرجشون کرد.

ولی هنوز اون خروجی هایی که بلااستفاده برگشت خوده به حساب یا باقیمانده در حساب هستند قابل استفاده می باشند، که درواقع اون ها رو با تراکنش های خرج نشده و قابل استفاده نام گذاری می کنیم که مخفف آن می شود (UTXOs).

مقدار کل تعداد بیت کوین های داخل یک حساب برابر هست با مجموع کل همین UTXOs های حساب.

ببینید میایم مثلا مقادیر  $[1] + [0.5] + [2] + [1]$  رو که به عنوان خروجی هستند رو برای ورودی یک معامله می خواهیم انجام بدهیم. اما مسئله ای که داریم اینه که مجموع مقادیر بیشتر از مقداری هست که ما می خواهیم ارسال کنیم!

حالا ما می تونیم در اینجا هر نوع ترکیبی از این خروجی ها رو ایجاد کنیم، ینی (هر ترکیب خروجی، ورودی مورد نظر) مورد نظر رو بوجود میاریم.

$$\begin{aligned} [1] + [3] + [0.5] &= 4.5 \\ [3] + [2] &= 5 \\ [1] + [3] + [0.5] + [2] + [1] &= 7.5 \end{aligned}$$

همه اینها مناسب هستند، شما می توانید برای خود تغییرات مورد نظر خودتون رو اعمال کنید.

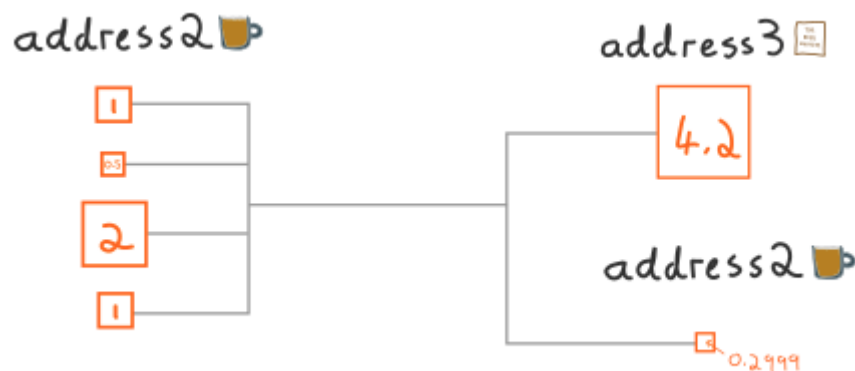
### تراکنش 3 – کارمزدهای (هزینه ها) معاملات

در تراکنش های انجام شده مقداری برای کارمزد یا همان هزینه تراکنش ها وجود داره که نیاز به بررسی آن ها می باشد.

بدون اینکه هزینه تراکنش رو پرداخت کنید، معاملات شما همه گی در یک بلوک اضافه می شوند، این بخاطر اینه که هزینه یک معامله اولویت انجام شدن تراکنش شما رو نشون میده.

کارمزد همان مقداری هست که استخراج کننده برای انجام دادن عملیات تراکنش شما از شما دریافت می کنه، بنابراین برای انگیزه به ماینر (استخراج گر) که یک تراکنش رو بزاره داخل یک بلوک این نوع هزینه قرار داده شده است.

فرض می کنیم تراکنشی رو انجام داده ایم و هزینه اون رو هم در نظر گرفته ایم و در شبکه فرستادم.



وقتی ما یک تراکنشی میزنیم از خروجی های خودمون که به ورودی های یک بالانس دیگه اضافه بشه، مقداری بیت کوین رو میفرستیم و کلا کار ترکیبات خروجی رو انجام میدیم (اینکه به چه شکلی از ترکیب این خروجی



انجام بگیره)، اما اون وسطا خروجی کارمزد رو نمیبینیم، ولی اگه توجه کنیم به مقادیری که از حساب خارج شده؛ میبینیم مقدار قبل از کم شدن بزرگتر از مقدار پس از انجام تراکنش هست! این همون مقدار کم که بوجود میاد، همون میزانیه که کارمزد هست و ماینر می تونه بنام خودش تراکنش رو ثبت کنه و برداره.

مجموع خروجی ها کمتر از مجموع ورودی ها هستش، و این ینی اینکه مقداری از بیت کوین هایی که مصرف نشده اند باقی می مانند، این مقداری هست که بیش از حد هزینه معامله هستش.

مبلغ اضافه ای که می مونه از (ورودی - خروجی) همیشه توسط ماینر برداشته می شه، بنابراین اگه یکوقت یک تراکنش دستی انجام دادید و فراموش کردید که یک خروجی برای خودتون تعریف کنید، اون موقع ماینر اون مبلغ (که مهم نیست چه مقداری هستش) که فراموش کردید برای خودش انتخاب می کنه.

❖ برگرداندن بعضی جملات انگلیسی به فارسی کار سخته، اگه جایی بد مفهومی پیش اومد، از روی متن اصلی بهتر می تونید متوجه مقصود حرف بشید.

Source: <http://learnmeabitcoin.com/guide/outputs>

و اینجا آخر این قسمته!  
شاد زی..