比特幣金流簡介

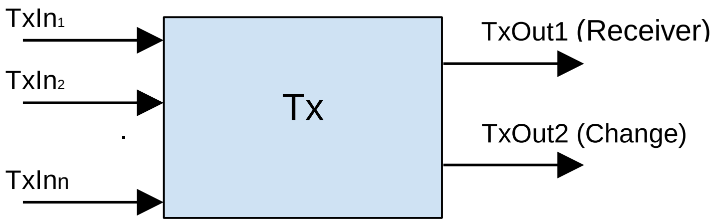
金流

比特幣的金流有別於我們一般對一個電子錢包的認知，以往我們談到電子錢包，就是我們錢包裡有多少錢，交易(Transaction, Tx)發生時，就轉移多少的錢給對方。然而比特幣的運作模式，反而比較像是傳統的錢包，錢在錢包裡比較貼近於各種不同面額的貨幣，這些不同面額的貨幣，我們稱之為Unspent Transaction Output (UTxO)，在交易發生時，會從錢包裡收集足量的UTxO之後，再轉送給對方，多餘的部分以找錢的方式轉送回自己的錢包中，用這樣的方式來完成交易。下面透過一個例子來幫助大家理解。

Alice有一個比特幣錢包，在先前的交易中，讓Alice的錢包中有數個UTxO，分別是1BTC、0.5BTC、0.7BTC。Alice想向Bob以1.2BTC買Bitcoin會議的門票，這時候建立一筆交易使用1BTC和0.5BTC轉送給Bob，Bob就會得到1.2BTC的UTxO，Alice手上就剩下0.3BTC和0.7BTC的UTxO。

交易

有了UTxO的概念之後，我們可以開始釐清交易是如何發生的。每一筆交易行為的紀錄，直觀的是將錢轉送到另一個錢包的過程。在比特幣的架構中，收送的單位我們稱之為地址(Address)，地址的產生是藉由公開金鑰加密的演算法，一把私鑰可以經過一個單向函式得到公鑰，公鑰可以得到地址。也就是說，在比特幣的架構之下，交易就是每個（數個）UTxO傳送到另一個地址的紀錄。因此某一個地址所擁有的餘額，就是他的UTxO的總和，值得一提的是，每個錢包是可以擁有複數個地址的，地址也可以自由產生，因此找錢的不需要是原本付錢的地址，而一個人（錢包）擁有的總財產就是所有的地址的餘額總和。



綜上所述，一筆交易的結構如上圖所示。在前面所提到的UTxO本質上就是某一個交易輸出(TxOut)，裡面包含了對應的金額、以及用於簽章以證明對此UTxO擁有權的公鑰資訊。交易輸入(TxIn)端的部份記錄包含了所使用的UTxO以及簽章的資訊，利用簽章配合UTxO的公鑰就可以驗證所有權。藉由這種TxIn對應到另一筆交易的TxOut的方式，可以將一筆一筆的交易串接起來，進而建構出比特幣的金流。又交易是以這樣的方式串接起來的，因此往回追溯之後必定會有一個源頭，是沒有輸入端的交易，這樣的交易稱之為Coinbase Tx，它就像是鑄幣一樣，會讓整個系統的總貨幣量增加，是一種十分特殊的交易，也因此他的產生格外嚴格。

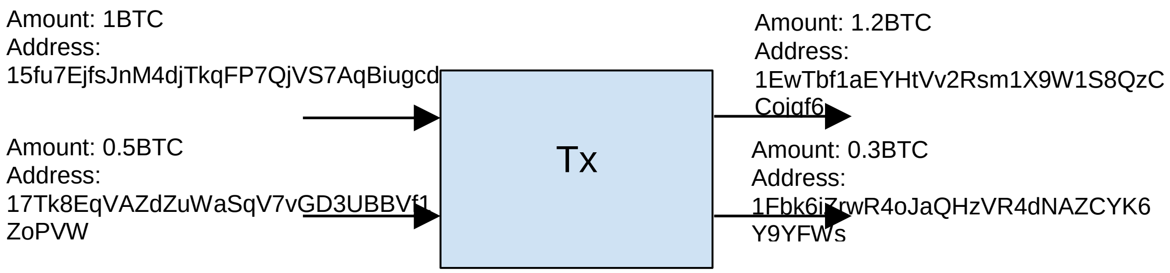
回頭看剛剛Alice和Bob的例子，假設Alice原本手上的三個UTxO分別位於三個地址：

1BTC：15fu7EjfsJnM4djTkqFP7QjVS7AqBiugcd

0.5BTC：17Tk8EqVAZdZuWaSqV7vGD3UBBVf1ZoPVW

0.7BTC：1AQG23ZsdwM1zvTVWkAEtsNpr2UArTgq4L

而 Bob 提供的地址為 1EwTbf1aEYHtVv2Rsm1X9W1S8QzCCojqf6，Alice 希望找錢的地址為 1Fbk6iZrwR4oJaQHzVR4dNAZCYK6Y9YFWs，那麼在不考慮手續費的狀況下，交易就會包含下列資訊：


Amount: 1BTC
Address:
15fu7EjfsJnM4djTkqFP7QjVS7AqBiugcd
Amount: 0.5BTC
Address:
17Tk8EqVAZdZuWaSqV7vGD3UBBVf1
ZoPVW
Tx
Amount: 1.2BTC
Address:
1EwTbf1aEYHtVv2Rsm1X9W1S8QzC
Cojqf6
Amount: 0.3BTC
Address:
1Fbk6iZrwR4oJaQHzVR4dNAZCYK6
Y9YFWs

而交易結束後，Alice 手上的 UTxO 就轉為
0.7BTC：1AQG23ZsdwM1zvTVWkAEtsNpr2UArTgq4L
0.3BTC：1Fbk6iZrwR4oJaQHzVR4dNAZCYK6Y9YFWs

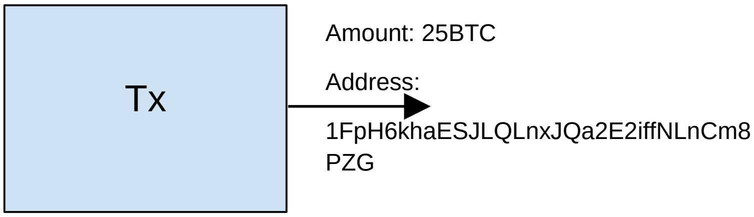
而 Bob 手上的 UTxO 則為

1.2BTC：1EwTbf1aEYHtVv2Rsm1X9W1S8QzCCojqf6

區塊

上面介紹完了比特幣上金流的概念，那這些交易是如何被記錄下來的呢？這就要提到比特幣的核心技術之一，也就是區塊鏈的區塊(Block)的概念。比特幣的網路每 10 分鐘會生產出一個區塊，每一個區塊在生產出來的時候必須記錄他前一個區塊的資訊，用這樣的方式把各個區塊串接在一起。上述的交易會在比特幣的網路中用廣播的方式傳播，等待被收進某一個區塊中，因此整條區塊鏈就如同一本帳冊，而每一個區塊就是其中的一頁。每個節點都有做出區塊的權利，而做出區塊並成功接上區塊鏈的使用者，會得到一定金額的獎勵，因此這樣的行為就像是挖礦(Mining)一般，這樣的使用者則稱為礦工(Miner)，而這個獎勵就稱為 Mining Award，這個獎勵的金額會在比特幣的機制中有嚴格的規範，在經過一定的時間之後就會減少，因此整個網路上的比特幣總額是有限的，就如同礦藏會有開採完畢的一天。Mining Award 會透過前段所述的 Coinbase Tx 轉送到該使用者的地址，這也是唯一會出現 Coinbase Tx 的地方。

假設今天 Charlie 是一個礦工，並且成功造出了一個區塊接到比特幣網路上，那麼他造出的區塊第一個交易就會是一筆 Coinbase Tx 送到他的地址，假設 Charlie 的地址是 1FpH6khaESJLQLnxJQa2E2iffNLnCm8PZG，那就這筆交易包含的資訊如下：



這也就會讓 Charlie 得到一個 25BTC 的 UTxO。

Bitcoin Flow Introduction

Bitcoin flow

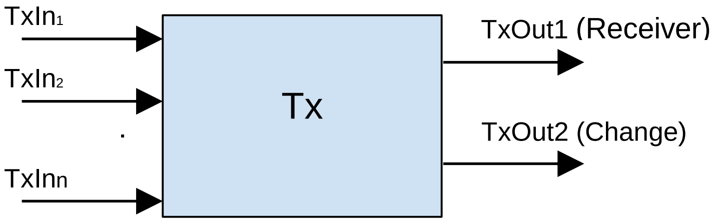
The “cash flow” of Bitcoin is a little different from the common image when we talk about digital currency. For the general idea of digital currency, the exact amount should be deducted from a wallet, and the same amount should be added in the receiver’s wallet. However, the mechanism of Bitcoin is more similar to the idea of the "real wallet”. The “money” in the Bitcoin wallet are coins with different face value. These coins are called the UTxO, the Unspent Transaction Output. When a transaction happens, the sufficient amount of UTxO will be collected and transferred to the receiver. The extra amount will then be transferred back to the sender as a change.

For example, Alice has a Bitcoin wallet, which has several UTxOs from earlier transactions. The UTxOs are 1 BTC, 0.5 BTC and 0.7 BTC. Alice wants to buy a ticket of Bitcoin conference for 1.2 BTC. A transaction will be carried out by using the UTxOs that are 1 BTC and 0.5 BTC. Bob will then receive 1.2 BTC, which becomes his new UTxO. The extra 0.3 BTC will be returned to Alice as a change. Therefore, Alice will have two UTxOs that are 0.3 and 0.7 BTC after this transaction.

Transactions

With the concept of UTxO, let’s consider how transactions can take place. Each transaction is a process where a certain amount of money is transferred from one place to another place. With the terminology of Bitcoin, the places where cryptocurrencies are sent or received are called addresses, which are generated with the hash algorithm based on public keys. To put it in Bitcoin terms, a transaction is a record which states a certain amount of UTxO is transferred from one address to another. And the balance of an address is the sum of all the UTxOs owned by the address.

Please note that each wallet can have multiple addresses which can be generated freely. The address used to pay money and the address used to save the change need not to be identical. And the total assets of a person’s wallet equal the sum of the balances of all the addresses inside the wallet.



The picture above illustrates what a transaction looks like. The aforementioned UTxO, by itself, is a transaction output (TxOut), which records amount and public key used as validate the ownership. A transaction input (TxIn) records the spent UTxO and the signature. By combing the signature and the public key, the ownership of the UTxO can be validated. By associating a TxIn with a TxOut of another transaction, the transactions can be linked together, forming a Bitcoin flow. With this structure, transactions can be traced back to an origin where no TxIn exists. Such transactions without TxIn are named Coinbase Tx, which are very special as they can increase the overall supply of cryptocurrencies, much like coining money in real world. Hence, strict rules apply to how Coinbase Tx can be generated.

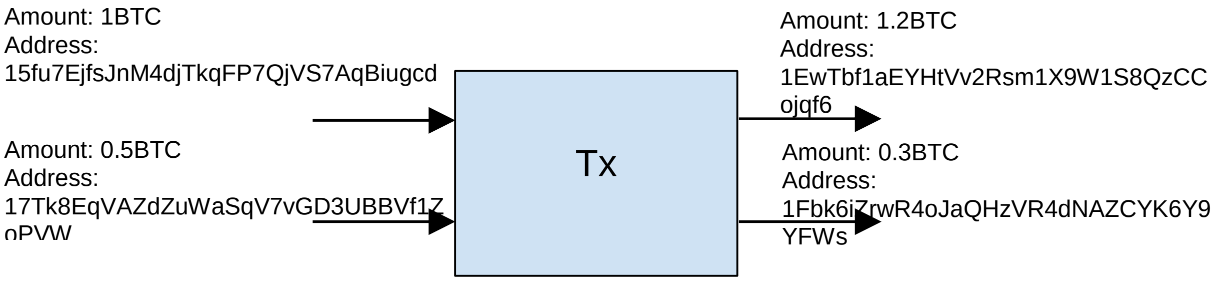
Let's go back to the previous example. Suppose Alice have three UTxOs located at three addresses:

1BTC：15fu7EjfsJnM4djTkqFP7QjVS7AqBiugcd

0.5BTC：17Tk8EqVAZdZuWaSqV7vGD3UBBVf1ZoPVW

0.7BTC：1AQG23ZsdwM1zvTVWkAEtsNpr2UArTgq4L

And the address provided by Bob is 1EwTbf1aEYHtVv2Rsm1X9W1S8QzCCojqf6. The address where Alice would like to store the change is 1Fbk6iZrwR4oJaQHzVR4dNAZCYK6Y9YFWs. Omitting the transaction fee, the transaction will look like the illustration as below:


Amount: 1BTC
Address:
15fu7EjfsJnM4djTkqFP7QjVS7AqBiugcd
Amount: 0.5BTC
Address:
17Tk8EqVAZdZuWaSqV7vGD3UBBVf1Z
oPVW
Tx
Amount: 1.2BTC
Address:
1EwTbf1aEYHtVv2Rsm1X9W1S8QzCC
ojqf6
Amount: 0.3BTC
Address:
1Fbk6iZrwR4oJaQHzVR4dNAZCYK6Y9
YFWs

After the transaction, the UTxO owned by Alice will be changed to:

0.7BTC：1AQG23ZsdwM1zvTVWkAEtsNpr2UArTgq4L

0.3BTC：1Fbk6iZrwR4oJaQHzVR4dNAZCYK6Y9YFWs

While the UTxO owned by Bob will be changed to:

1.2BTC：1EwTbf1aEYHtVv2Rsm1X9W1S8QzCCojqf6

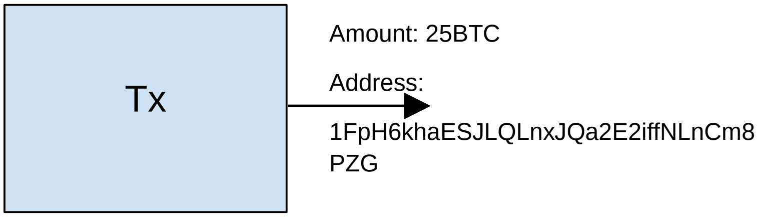
Block

The above describes the concept of Bitcoin flow on the Bitcoin blockchain. But how are these transactions recorded? It is necessary to mention one of Bitcoin's core technology, which is the "block" concept.

Bitcoin network produces a block every 10 minutes, each block has record of the information of previous block, and in such way the blocks are linked chronologically. Every transaction is broadcast in the network, and miners record the transaction in the block. This process makes blockchain a distributed ledger, and each block is like a page of this ledger book. Each node has the right to make blocks, and nodes that successfully make the block which is connected to other nodes will be rewarded a certain amount of coins, so this behavior is called "mining", and the node is called the "miner", and the reward is called the "mining reward".

The amount of mining reward has strict rules in Bitcoin protocol, which will decrease in half after a period of time, so the total amount of Bitcoin has a upper limited, just like most mineral resources have their amount of reserve. Mining reward is transferred to the miner's address through the coinbase transaction, which is the first transaction of every block.

For example, Charlie is a Bitcoin miner who successfully create a block connected to the Bitcoin network, then the first transaction of the block he made is the coinbase transaction with output to his address. Assume Charlie's address is 1FpH6khaESJLQLnxJQa2E2iffNLnCm8PZG, the coinbase transaction would include the following information:



Thus, Charlie will earn 25BTC of UTxO from this transaction.