UTXO (Unspent Transaction Output)

Smita Kulkarni-Pai

What Are the UTXO and Accounts Models?

- Both the UTXO (unspent transaction output) and accounts models are methods of cryptocurrency record-keeping used to represent the number of tokens someone has remaining after executing a **transaction** on the blockchain.
- These models are a key method in which blockchain architecture maintains an accurate ledger while ensuring privacy.

1. UTXO Model

- The easiest analogy for UTXOs is physical **fiat currency**. Just like how coins or notes cannot be split into smaller denominations, a UTXO cannot be divided either.
- One can think of a UTXO as a discrete (indivisible and unique) chunk of its corresponding token controlled by the **private key** of its owner.
- The UTXO model is used by projects such as Bitcoin (**BTC**), Bitcoin Cash (**BCH**), Litecoin (**LTC**), and Zcash (**ZEC**) among others.

UTXO

- The collection of all existing UTXOs at any given point is called the *UTXO set*. Any transaction performed on the blockchain can be viewed as a modification of the UTXO set.
- Example of fiat currency collection : lets say Alice has following collection of notes (Alice Cash Details)

10 Rs notes x 10	50 Rs notes x 5	100 Rs Notes x 10	500 Rs Notes x 5	Total Rs
100	250	1000	2500	3850

UTXO

➔ Alice has to give Bob Rs 250. Let's say Bob already have 2500 Rs.

Alice Cash	
total	3850
Dr to Bob	3x100 →
Received from Bob	50
Remaining (Unspent)	3600

UTXO generated

300 + 50

Total amount in channel

BoB Cash	
total	2500
Cr from Alice	300
Return to Alice	50 ←
Remaining (Unspent)	2750

How Does a UTXO Transaction Work?

UTXO model blockchains execute transactions by using UTXOs generated by previous transactions as an input, then receive UTXOs generated by the new transaction as an output.

Transactions under the UTXO model can be understood through the following example:

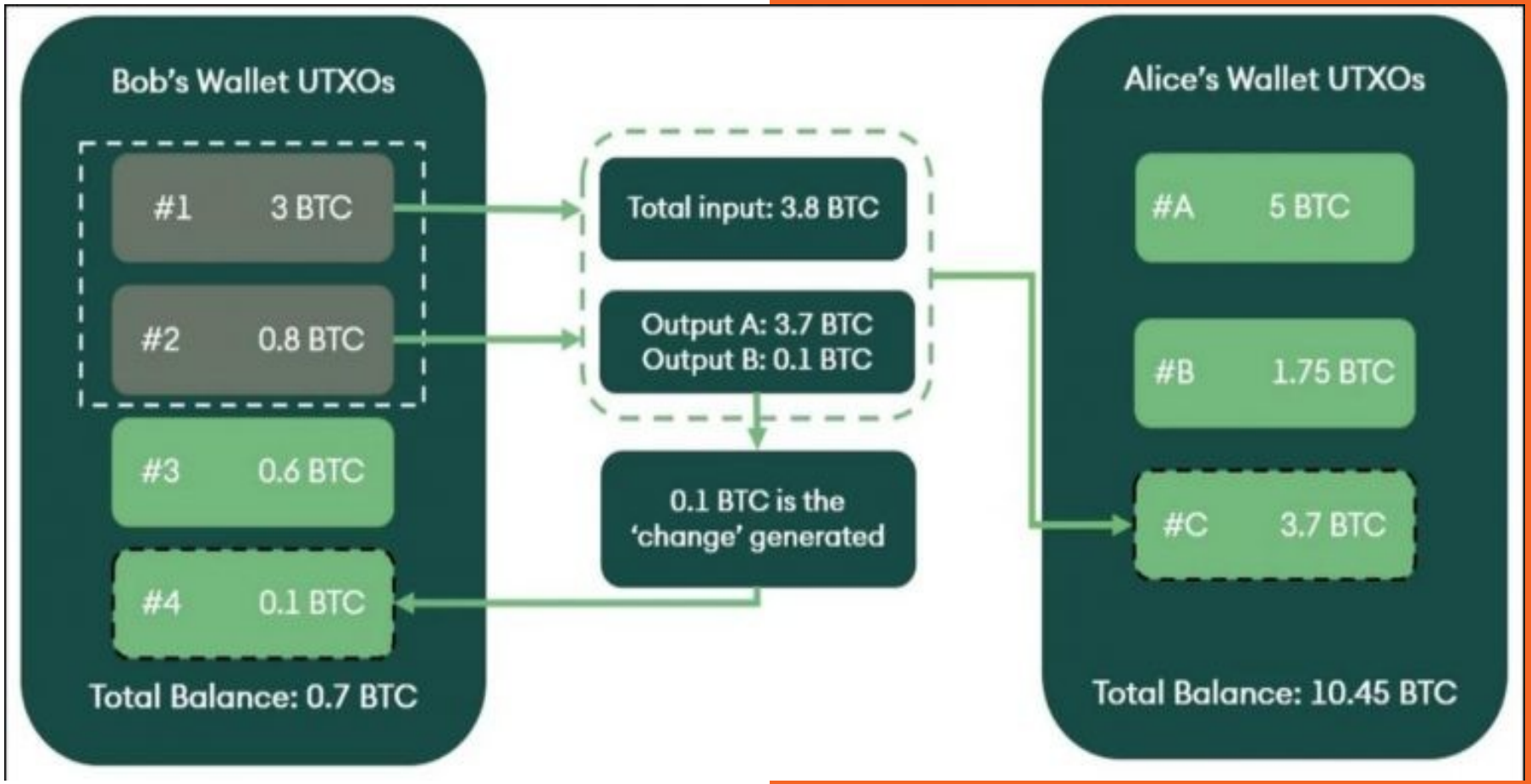
- Bob has three $20 notes. Each note represents a single UTXO. They cannot be exchanged for smaller denominations without first being “consumed.” For example, to exchange a $20 note for two $10 notes, Bob must *consume* the UTXO representing $20 for two UXOs representing $10 each.
- Bob wants to pay Alice $35.
- Bob hands Alice two $20 notes, then receives one $5 note in return.
- A total of two UTXOs were generated in this transaction. The first represents the two $20 notes given to Alice, while the second the $5 in change given back to Bob.

Unlike physical currency, a single UTXO could represent 5 BTC, 479.2 BTC, or anything in between.

The tokens held in a user’s wallet represent the total amount of UTXOs under their ownership. Moving onto the blockchain, let’s instead consider what would happen if Bob wanted to send Alice 3.7 BTC:

UBob’ s wallet contains a total of three UTXOs, valued at 3 BTC, 0.8 BTC, and 0.6 BTC respectively. These UTXOs will be used as the input for this transaction, and were themselves output from a previous transaction.

- As Bob does not have enough BTC in a single UTXO to cover the transaction, he sends both the 3 BTC and 0.8 BTC UTXOs to Alice, representing a total of 3.8 BTC.
- The two UTXOs are consumed. Alice’ s wallet receives a new UTXO of 3.7 BTC, while Bob’ s wallet receives a new UTXO with the remaining 0.1 BTC.



Visual representation of a UTXO model transaction (Source: SEBA Bank Research)

2. Account Model

- The easiest analogy for the account model is a debit card or bank account.
- Unlike physical fiat currency that cannot be split into smaller denominations, an account model supports the credit (or debit) of any arbitrary amount of the token.
- While UTXO wallets represent the total sum of a user’s UTXOs, an account model wallet simply represents the user’s aggregate balance.

2. Account Model

- The easiest analogy for the account model is a debit card or bank account.
- Unlike physical fiat currency that cannot be split into smaller denominations, an account model supports the credit (or debit) of any arbitrary amount of the token.
- While UTXO wallets represent the total sum of a user’s UTXOs, an account model wallet simply represents the user’s aggregate balance.

How Does an Account Model Transaction Work?

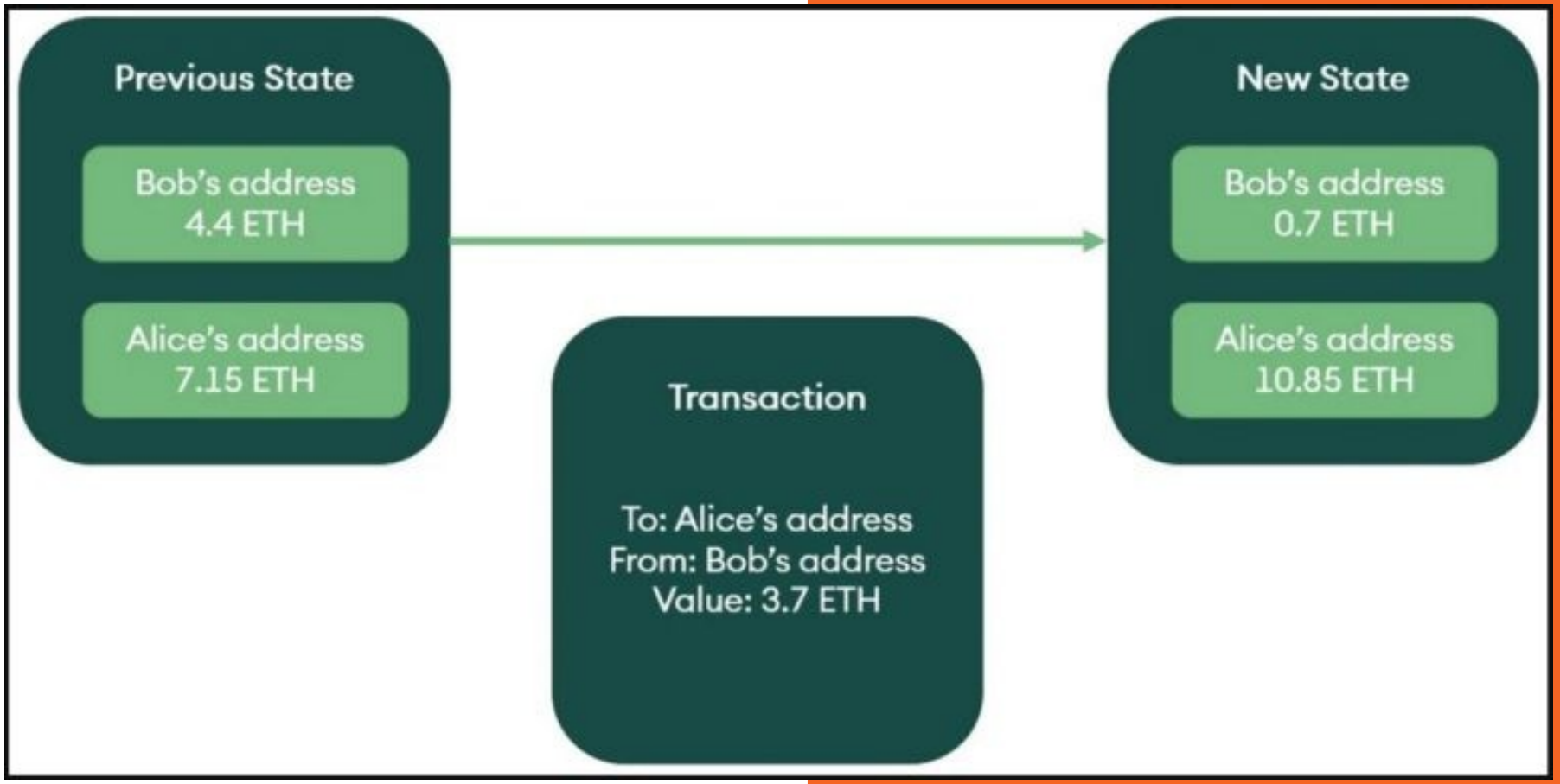
The balance of each account is stored on the blockchain.

Account model blockchains execute transactions simply by reducing the balance of one account, then increasing the balance of the recipient by the corresponding amount.

How Does an Account Model Transaction Work?

Let’s see how the previous example would differ if Bob instead wanted to send Alice 3.7 ETH.

- Bob’s wallet contains a single balance of 4.4 ETH.
- As Bob’s wallet is a singular balance, he can directly transfer 3.7 ETH to Alice.
- The 3.7 ETH is deducted from Bob’s wallet and added to Alice’s wallet.



Visual representation of an account model transaction (Source: SEBA Bank Research)

What Is Double-Spending?

Double-spending is spending the same cryptocurrency or blockchain token more than once.

Cryptocurrency is a token that represents value on a distributed ledger, so without proper mechanisms in place it, would be easy to change a ledger entry and give yourself back the amount you had spent.

Double Spending Attacks

The most significant double-spending risk for blockchains is a 51% attack, which can occur if an entity controls more than 50% of the hashing power or validation mechanisms on a network.

If this user—or users—assumes a majority of the network, the network's stake, or any other mechanism used, they will be able to dictate transaction consensus and control the award of currency.

Preventing Double Spending

The solution presented by Satoshi Nakamoto, which involved timestamping transactions and chaining them together using cryptographic techniques, solved the double-spending problem.

Various consensus mechanisms can be used to prevent double spending.

Reference

https://phemex.com/academy/what-are-utxo-unspent-transaction-output

https://www.investopedia.com/terms/d/doublespending.asp