
# UTXO Model Vs Account Model

# Transaction - UTXO Vs Account Model

It is necessary for a digital money to be transferable in order for it to be useful. The transaction is created when the owner initiates the transfer of funds on a blockchain. This transaction informs the network of the amount of money changing hands and the identity of the new owner.

Blockchain's sole purpose is to keep track of past events and user interactions.

The system goes through a state transition with each new block.

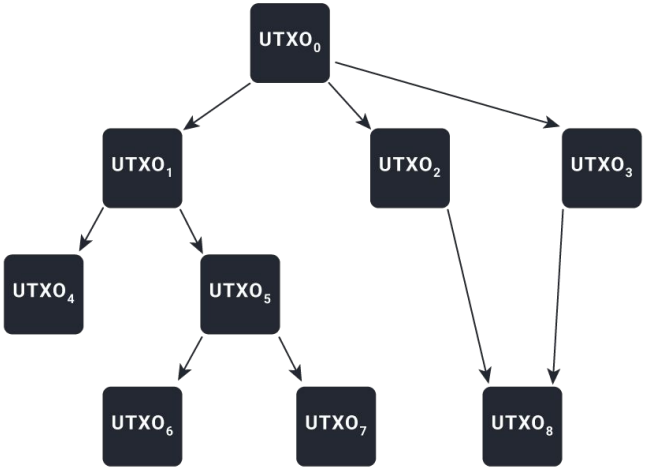
Any blockchain, regardless of whether it follows the UTXO or account model, goes through a state transition.

The user interactions, which are mainly transactions, are broadcasted to the network, and a set of them are recorded forever with each new block.

When the system transitions to a new state, the balances of the transacting parties are updated.

# UTXO Vs Account Model

**UTXO Model**




**Directed graph of assets(UTXOs) moving between users**

**Account Model**

| | | |
|---|---|---|
| State n | Account A | Balance $t_0$ |
| State (n+1) | Account A<br>Account B | Balance $t_1$<br>Balance $t_1$ |
| State (n+2) | Account A<br>Account B | Balance $t_2$<br>Balance $t_2$ |
| State (n+3) | Account A<br>Account B<br>Account C | Balance $t_3$<br>Balance $t_3$<br>Balance $t_3$ |

**Database of network states**

# UTXO Model

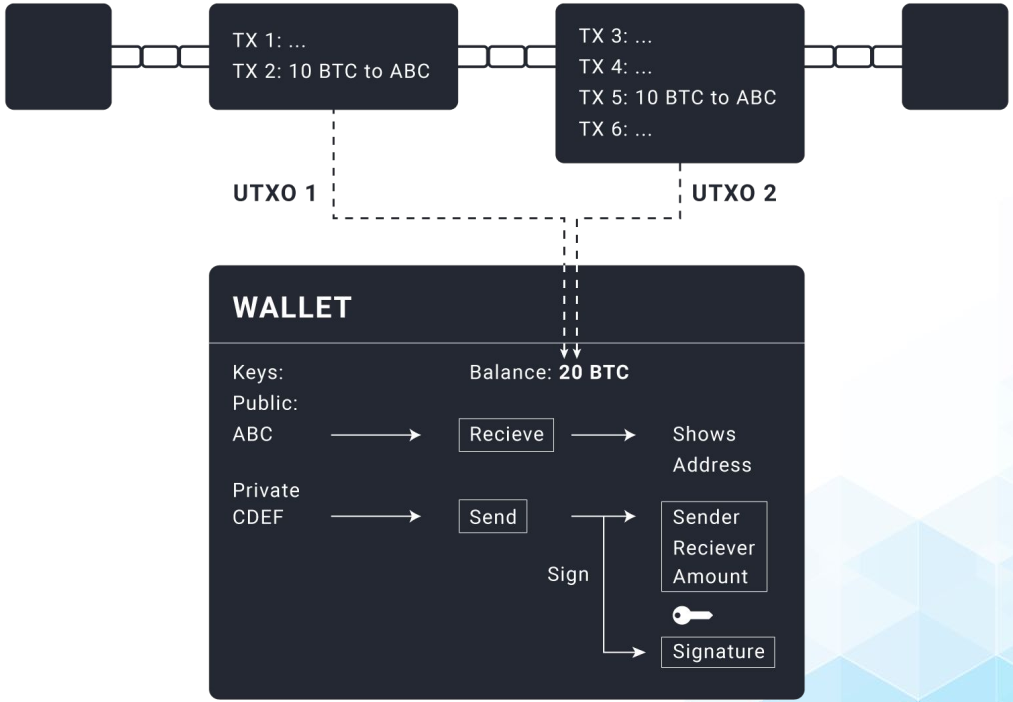
At the protocol level, the UTXO model is devoid of accounts and wallets. Individual transactions, clustered into blocks, form the basis of the model. This can be compared to those who have a certain amount of cash in their possession.

- A user with 50 BTC may have control over a single UTXO worth 50 BTC or a collection of UTXOs worth 50 BTC
- If a person has $50 in currency, he might have a single $50 bill or a mixture of smaller denominations.

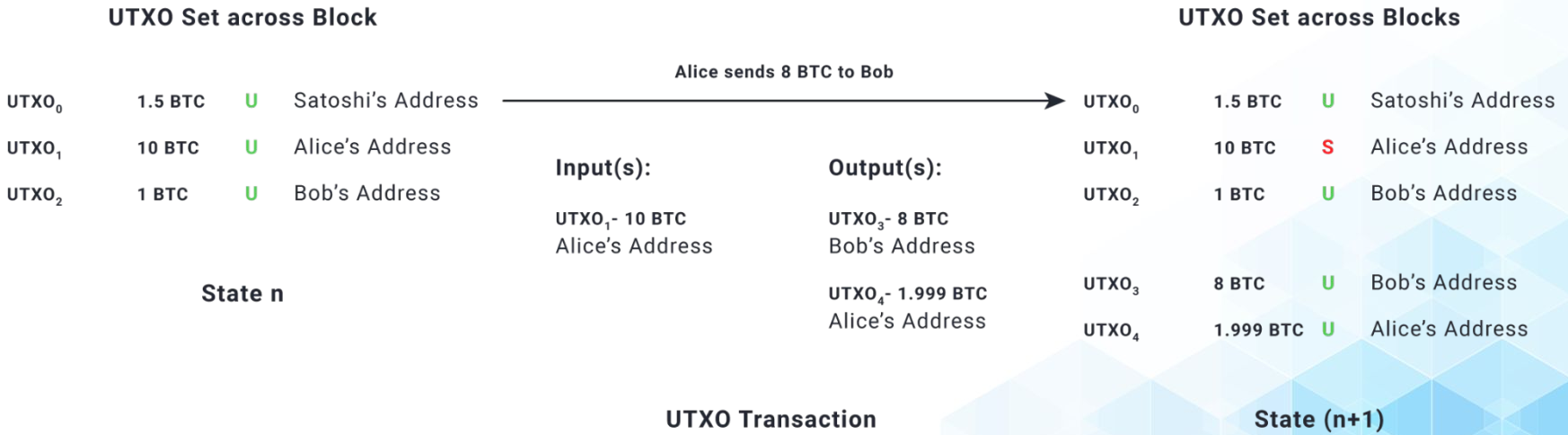
When a user does not wish to transfer the whole amount of a UTXO, the difference between the UTXO size and the amount the user is willing to spend is transmitted as a change to a self-controlled address.

- Spending 10 BTC from a 50 BTC UTXO results in two outputs in the transaction: a 10 BTC output to the payee and a 40 BTC shift output to the original owner.
- Spending $10 on a $50 bill entails sending the money to the payee and getting $40 in change in exchange.

# UTXO Model



# State Transitions in the UTXO Model



# Account based Model

In the account-based transaction model, assets are represented as balances inside accounts, equivalent to bank accounts. This transaction model is used by Ethereum. There are two kinds of accounts:

- Private key controlled user accounts
- Contract code-controlled accounts

In the account-based paradigm, a transaction causes nodes to decrement the sender's account balance and increase the receiver's account balance. Each transaction in the account model has a nonce tied to it to avoid replay attacks. When a payee broadcasts a fraudulent transaction, they are paid twice.

In order to resist this behavior, each account in Ethereum has a public viewable nonce that is incremented by one with each outgoing transaction. This stops transfers from being sent to the network several times.

# State Transitions in the Account Model