Overview of UTXO

* *Ish Handa*

UTXO (Unspent Transaction Output)

It is the input of a transaction in a valid blockchain payment system. Each transaction included the exhaustion of previously generated UTXOs and creation of new ones to be used in the future.

An UTXO basically represents where a coin is at that current moment.

Benefits

Scalability and Parallel transactions: When a sender created two transactions, they are dealt with separately, however these transactions are can also be processes in any order and thus provide scalability.

Disadvantage

Complicated: UTXOs create complication, which is not required as per say and they complicate the implementation

Stateless: UTXOs are stateless and thus do not have applications dealing with smart contracts.

Accounts, an alternative way

Accounts are like ledges, they store balances and codes. Just like a ledge, the transactions adopt a debit credit system for receiving and sending coins.

Advantages

Space Saving: Each transaction, only needs one reference and only produces one output thus not much space is used up.

Simplicity: In opposition of UTXO, an accounting system is easy to implement and understand.

Easy Querying: Like a ledger, the accounts table is easily scannable by a client.

Why UTXO over Accounts

Account systems can easily be affected by replay attacks; however, they handle it by attaching a nonce to each transaction, and the accounts keep a track of the nonces used. UTXO are more secure as they do not refer to one ledge table, but contain their own validated information(signature), which is cross validated each time a transaction happens. This is beneficial for a crypto-currency and thus is applicable here, but it might not be in other applications.