Basic Bitcoin Tech: UTXO Deep Dive 🤿

Host - SimplestBitcoinBook w/ PortlandHODL

- Overview -

- What is a UTXO?
- Analogy / Comparison
- UTXO Details
  - The coinbase UTXOs
  - Coinbase Transactions
  - Consolidation
  - Spending (Splitting)
  - Unspendable UTXOs (2 known)
  - UTXOs as a part of a transaction
- Coin Control and UTXOs
- Transactions vs. UTXOs

What is a bitcoin UTXO?

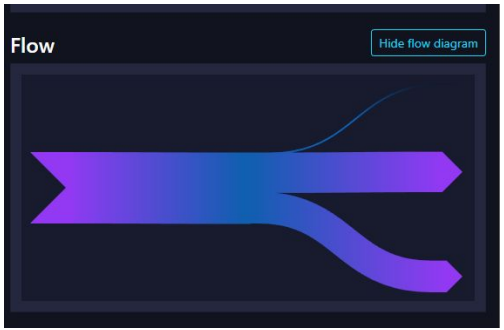
1. Definition

- UTXO stands for ‘Unspent Transaction Output’
- UTXOs represent all bitcoin that is spendable. As such all UTXOs equal the total supply.*
- A UTXO is a discrete single output (spend) of a bitcoin transaction.
- Many UTXOs can be included in a single transaction.

2. Notes

- In most monetary systems you have discreet denominations on notes. *E.g. $(1,5,10,20,100) a*nd a smallest unit of value *E.g. (Penny)*
- Due to the digital nature of bitcoin only the smallest unit is needed.
- As such the UTXO’s represent notes of an amount of the smallest unit of bitcoin. The digital nature of bitcoin lets us avoid having to combine sets of notes to make a value, instead the UTXO (note) becomes the value.

3. Visualized



A 1 -> 2 Transaction, Where one UTXO created 2 smaller UTXOs that when added together with the fee equal the original amount.

*There are unspendable UTXOs that do exist. They still count toward the total supply.

Coin, Money, and UTXOs - An analogy

FIAT 👎😔💩

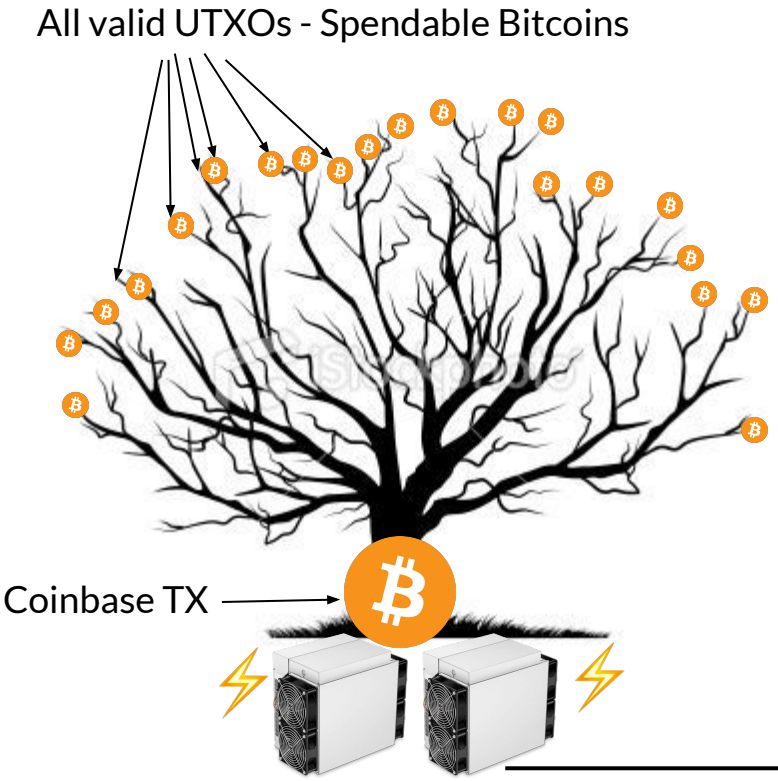
- **'The Fiat money exchange' example:** You have 75 cents (Three quarters) and want to buy a gumball for 59 cents. The only solution to pay for the gumball is to hand over your 3 quarters and receive 16 cents back; receiving a minimum 3 coins back a dime, nickel, and a penny. *(denominations can't be cut or clipped to create a new denomination)*

- **The Bitcoin standard example:** You have a 75 sat (UTXO) transaction in your wallet. The gumball is 59 sats. To purchase the gumball your take your 75 sat transaction and you create 2 new UTXOs (coins). One with a value of 59 sats and one with 16 sats. You keep the 16 sat UTXO and you sign the 59 sat UTXO to the seller. The final step once these funds have been spent from the original UTXO, is that the original UTXO is now made invalid. *Note that bitcoins can't be destroyed, they can only change UTXOs.*

The fact bitcoin isn't tangible is a benefit.

- Physical money needed to represent a 'state' of who owns what, and since no previous history is associated with coins and notes, each note needed to be instantly verifiable.
- As such there is a need to have a standardized set of notes and coins that can be exchanged between humans.
- This means letting users create bills that represent arbitrary and exact amounts of value isn't possible. *E.g. I may have 75 cents in three quarters, but it isn't possible to combine these units to make a 75 cent coin.*
- Since bitcoin is a digital ledger, the UTXO model allows users to create their own 'denomination' of sats as a UTXO because the network can always verify that the original UTXO is valid.
- Since there is no physical recombining of atoms it's very easy and convenient to just create a UTXO that is equal to the sum of the inputs. *E.g. I may have three 25 sat transactions, If I wanted to may a single 75 sat UTXO, I would just spend those three TXs into a single address. In one transaction.*
- Users can create their own denominations of the base unit (satoshi) because it can be verified at all times that the user didn't cheat and create or destroy coins.

UTXOs always trace back to a coinbase transaction.



- The only time bitcoins are ever created are in coinbase transactions, and no bitcoins are ever ‘destroyed’. *NOTE: A coinbase transaction can have multiple outputs (UTXOs)*
- If you look at a UTXO that your transaction was made from, and work backwards, you will eventually reach the creation of those bitcoin which is the UTXO(s) from the oldest coinbase transaction.
- ADVANCED NOTE: Coinbase UTXOs can be combined.

UTXO Consolidation

Many gold pieces melted into a larger bar

Combine 4 coins into a single note (4 UTXOs into 1)

UTXO consolidation is taking 2 or more UTXOs and combining them into 1 or more larger UTXOs. *A bitcoin transaction must take place on chain.*

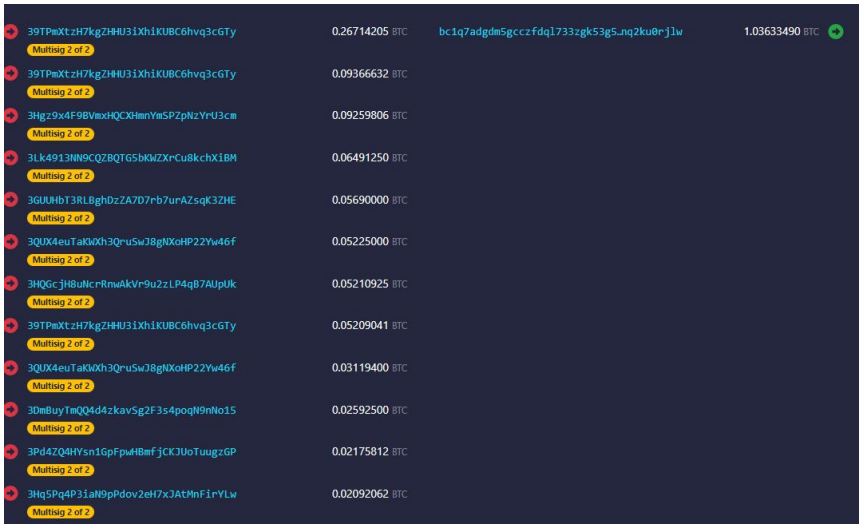
- FOR
  - Maskes UTXO management easier.
  - Reduces the TX fees when spending.
  - Makes it easier on nodes since the number of UTXOs in the set decreases.
  - Exchanges consolidate often to save on fees.
- AGAINST
  - Reduced privacy.
  - Takes a one time network fee to consolidate theses transactions.
  - Can completely compromise privacy if not careful. Hard to undo.

Do you value lower fees or privacy?

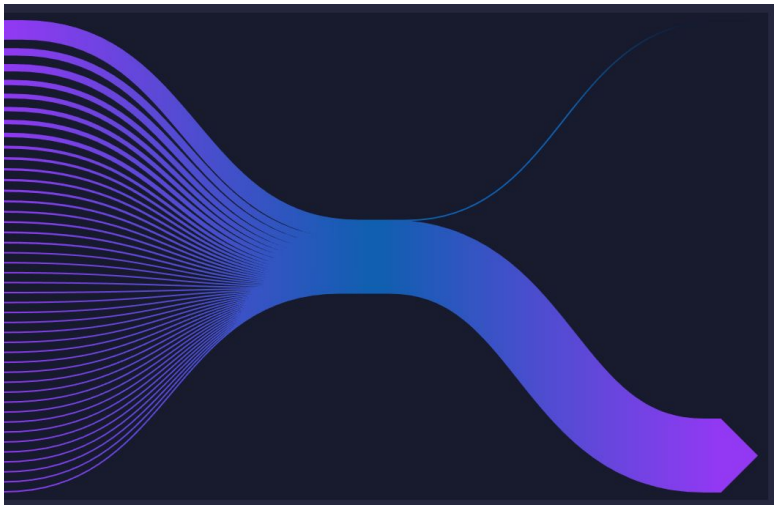
UTXO Consolidation visualized on Timechain Explorers

INPUTS = Many

Outputs = Few

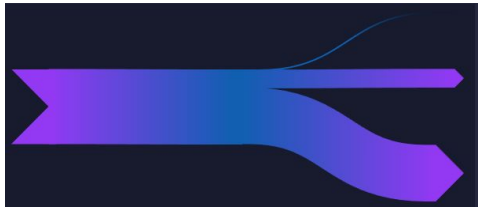


Input = Output + Fee



UTXO Splitting and Spending

4 pieces of a whole chocolate bar.



A single UTXO split into 2 + a fee.

Isn't talked about as much as consolidation but still can be useful.

- It can be useful to to split a UTXO into multiple pieces to store bitcoins in different locations or with different methods.
- Note: You don't obtain privacy by splitting a UTXO into pieces.
- Can be useful as a method to avoid exposing a larger amount of bitcoin while spending a smaller amount.
- An onchain transaction must be incurred to split up a UTXO
- Spending to a single recipient and receiving change to a single address will split a UTXO into 2 to smaller UTXOs.
- You can do this between two wallets you own.

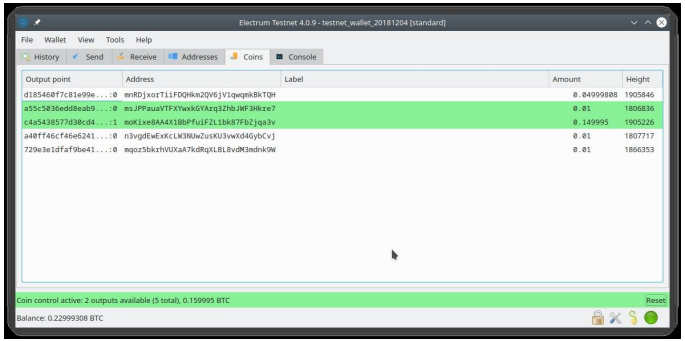
(Unspendable)TXOs

Locked Away Forever

Just a bit of bitcoin history.

- The coinbase reward of the genesis block is an unspendable UTXO This is 50BTC
  “4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b”
- All inputs(UTXOs) to address “1FYMZEHnszCHKTBdFZ2DLrUuk3dGwYKQxh” ~3.72BTC
  - Address generated with invalid exponents
  - Inputs are completely unspendable, ‘invalid’, not just burned to an address that doesn’t have a known key.
  - https://www.reddit.com/r/Bitcoin/comments/2t3vn0/i_cant_send_my_btc_a_triangle_apear_i_use_multibit/
  - Mathematically impossible to spend.

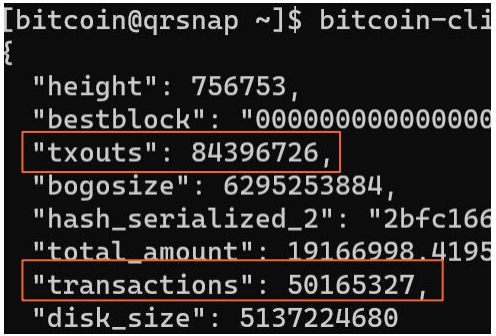
Coin Control and the UTXO.



Electrum Wallet Where the user selects ⅝ UTXOs available.

- Coin control is the act of managing UTXOs as to minimize fees and maximize privacy.
- This involves the selection of the UTXOs you want to include to build a transaction.
- An example where coin control comes into play would be where you are spending bitcoin that has no attachment to your identity, and you don't want to mix that transaction up with bitcoin that does have a tie to your identity.
- Wallets will mix transactions in the way they see best, and have no knowledge about your privacy. As such, wallets can often create transaction that leak information.
- Use multiple change addresses to throw off 'chainalysis'

Transactions Vs. UTXOs



Output of ‘gettxoutsetinfo’

- Since there can be multiple outputs to a single transaction, there will, with a high level of certainty always be more UTXOs than there are transactions.
- This can be seen with the Bitcoin Core command ‘gettxoutsetinfo’
- The ‘txouts’ value is the total number of UTXOs on the timechain
- The ‘transactions value is the number of transactions that carry these UTXOs
- Currently @ block 756753
  - 84,396,726 UTXOs
  - 50,165,327 Transactions

How UTXOs build a transaction ‘simply’

Transaction Inputs Format

Field	Description	Size
Previous Transaction hash	doubled SHA256-hashed of a (previous) to-be-used transaction	32 bytes
Previous Txout-index	non negative integer indexing an output of the to-be-used transaction	4 bytes
Txin-script length	non negative integer VI = VarInt	1 - 9 bytes
Txin-script / scriptSig	Script	<in-script length>-many bytes
sequence_no	normally 0xFFFFFFFF; irrelevant unless transaction's lock_time is > 0	4 bytes

- A transaction has N inputs and M outputs, *eg. 2 in 1 output* - That means you will be consuming 2 input UTXOs and creating a single output UTXO.
- The outputs UTXOs of transactions are ordered from 0 to M. When you want to spend a UTXO you must include the TXID of the transaction, and that order number (index of the specific UTXO that you would like to use)
- The outputs are just the UTXOs that will be created.

Thanks for listening!

1. Let us know what we can do better.
2. Anything incorrect? Leave a comment.