Blockchain Scripting Assignment part 3

Transaction Type	Size (bytes)	Virtual Size (vbytes)	Weight (WU)
Legacy (P2PKH)	225	225	900
SegWit (P2SH-P2WPKH)	215	134	533

Comparison Between Legacy P2PKH and SegWit P2SH-P2WPKH Transactions

1. Transaction Size Comparison

A clear difference can be observed in the transaction sizes between Legacy P2PKH and SegWit P2SH-P2WPKH transactions. The key details are summarized below:

Transaction Type	Size (bytes)	Virtual Size (vbytes)	Weight (WU)
Legacy (P2PKH)	225	225	900
SegWit (P2SH-P2WPKH)	215	134	533

Observation:
SegWit transactions consume significantly fewer virtual bytes and weight units compared to Legacy transactions. This results in more efficient use of block space.

2. Script Structure Comparison

Legacy (P2PKH)

- The **locking script (scriptPubKey)** contains standard instructions to verify a public key hash and check the signature.
- The **unlocking script (scriptSig)** carries both the signature and the public key required to unlock the output. This script appears directly in the main body of the transaction,

contributing to larger transaction size.

SegWit (P2SH-P2WPKH)

- The **locking script (scriptPubKey)** contains a hash pointing to a redeem script.
- The **unlocking script (scriptSig)** is minimal, as most of the unlocking data is moved to the **witness field**.
- The **witness field** contains the actual signature and public key required to satisfy the script conditions.

Key Difference:
In SegWit transactions, the unlocking data (signature and public key) is shifted from the main transaction body to the witness structure, reducing the effective size of the transaction.

3. Advantages of SegWit Transactions Over Legacy Transactions

Aspect	Legacy P2PKH	SegWit P2SH-P2WPKH
Unlocking Data Placement	Directly in scriptSig	In separate witness field
Virtual Size	Larger (225 vbytes)	Smaller (134 vbytes)
Weight Units	Higher (900 WU)	Lower (533 WU)
Transaction Malleability Fix	No	Yes
Fee Efficiency	Lower (higher fees)	Higher (lower fees)
Block Space Utilization	Less Efficient	More Efficient

4. Explanation of Size Reduction in SegWit

SegWit achieves size reduction by relocating the unlocking data to the witness field. The witness data is not counted fully towards the block size limit (only 1 weight unit per byte instead of 4 weight units per byte as in the main body). Consequently, the **virtual size** and **transaction weight** are reduced.

This leads to:

- **Lower transaction fees**: As fees are calculated based on vsize, smaller transactions incur lower costs.
- **Improved block capacity**: More transactions can fit into a block, increasing throughput.
- **Elimination of transaction malleability**: Since the signature is removed from the transaction hash calculation, it is no longer possible to alter a transaction's hash without invalidating the signature.

5. Conclusion

In summary, SegWit transactions offer substantial improvements over Legacy transactions in terms of size, efficiency, and security. The reduced size and fees, combined with enhanced scalability and transaction malleability protection, make SegWit the preferred choice in modern Bitcoin transactions.