SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 8:

Bitcoin – Part 3

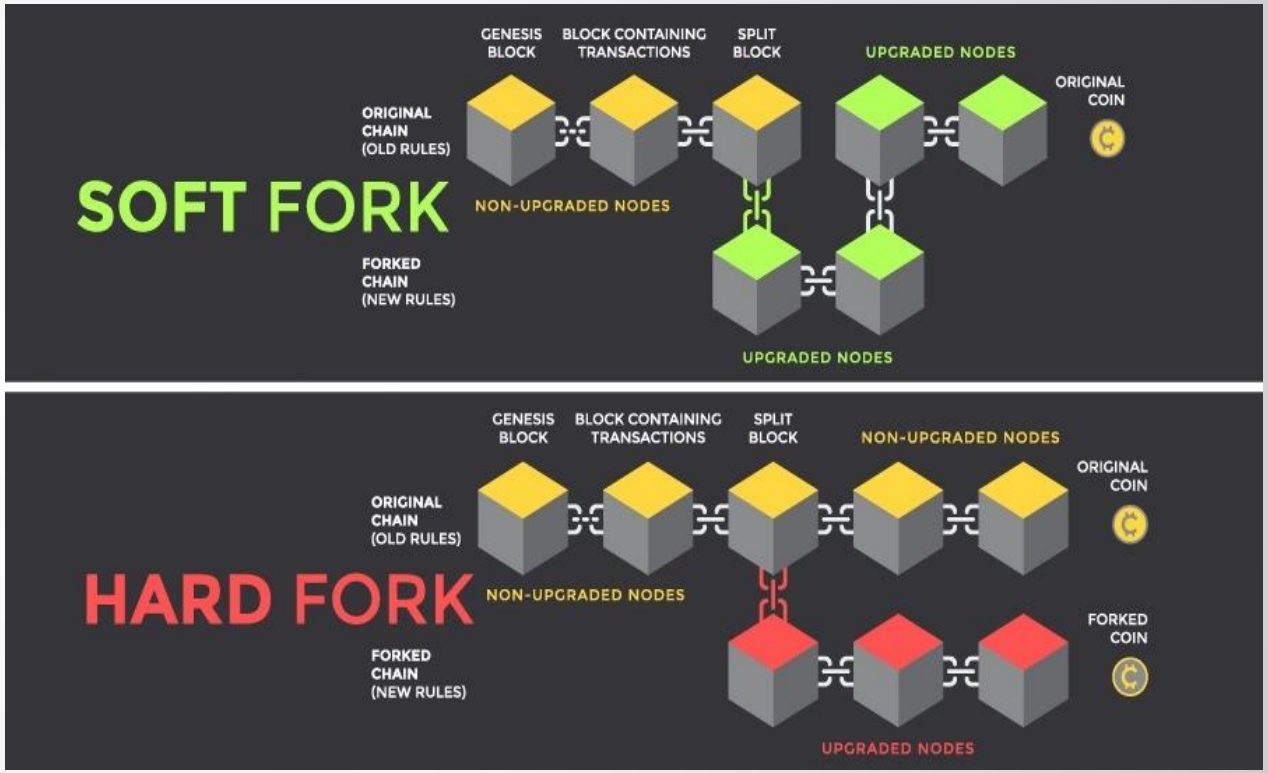
Module 1 – Segregated Witness

Sayad Haghighi

Soft Fork vs Hard Fork

Soft Fork: A soft fork is a backward-compatible upgrade to a blockchain protocol. It introduces changes that are compatible with the existing rules of the network, meaning that nodes running the updated software can still communicate and validate transactions with nodes running the old software.

Hard Fork: A hard fork is a backward-incompatible upgrade to a blockchain protocol. It introduces changes that are not compatible with the existing rules, resulting in a permanent divergence in the blockchain's history. A hard fork splits the blockchain network into two separate chains with separate histories.

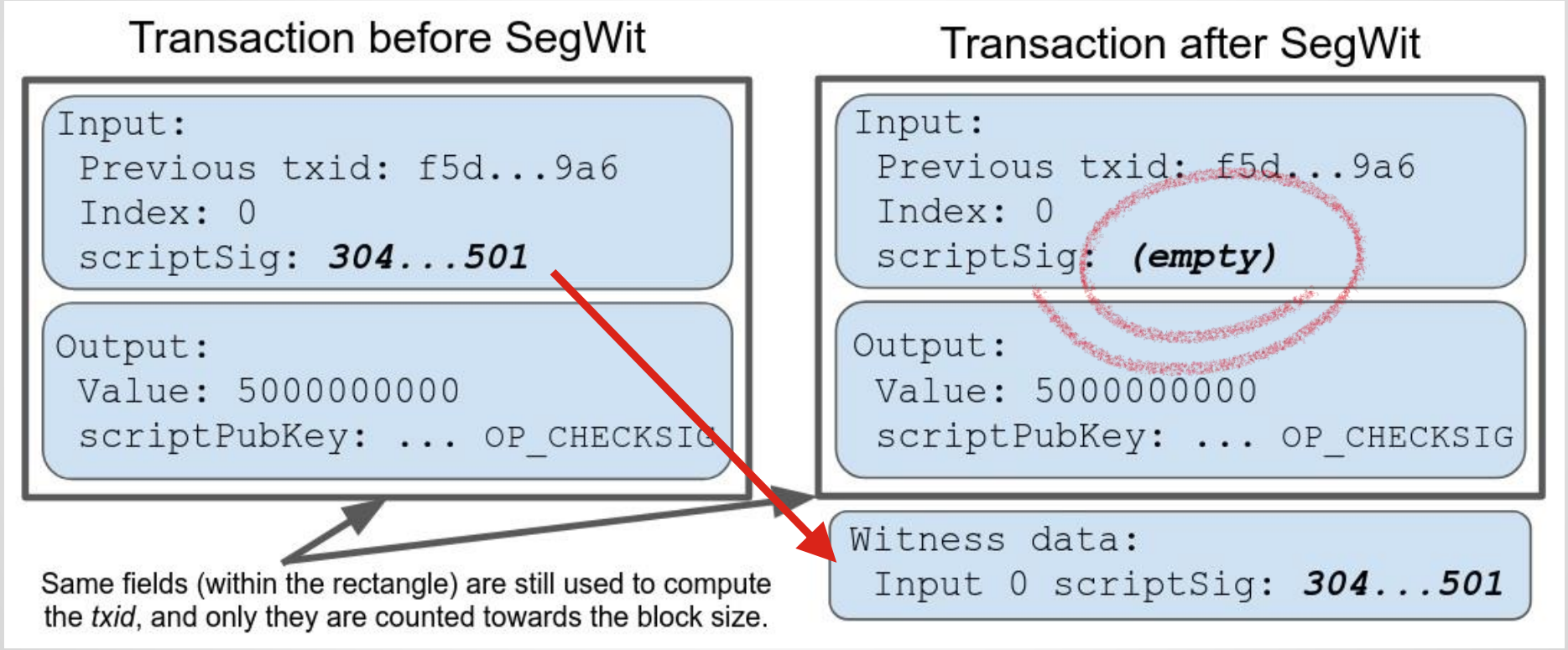


(www.financemagnates.com)

Segwit (Segregated Witness)

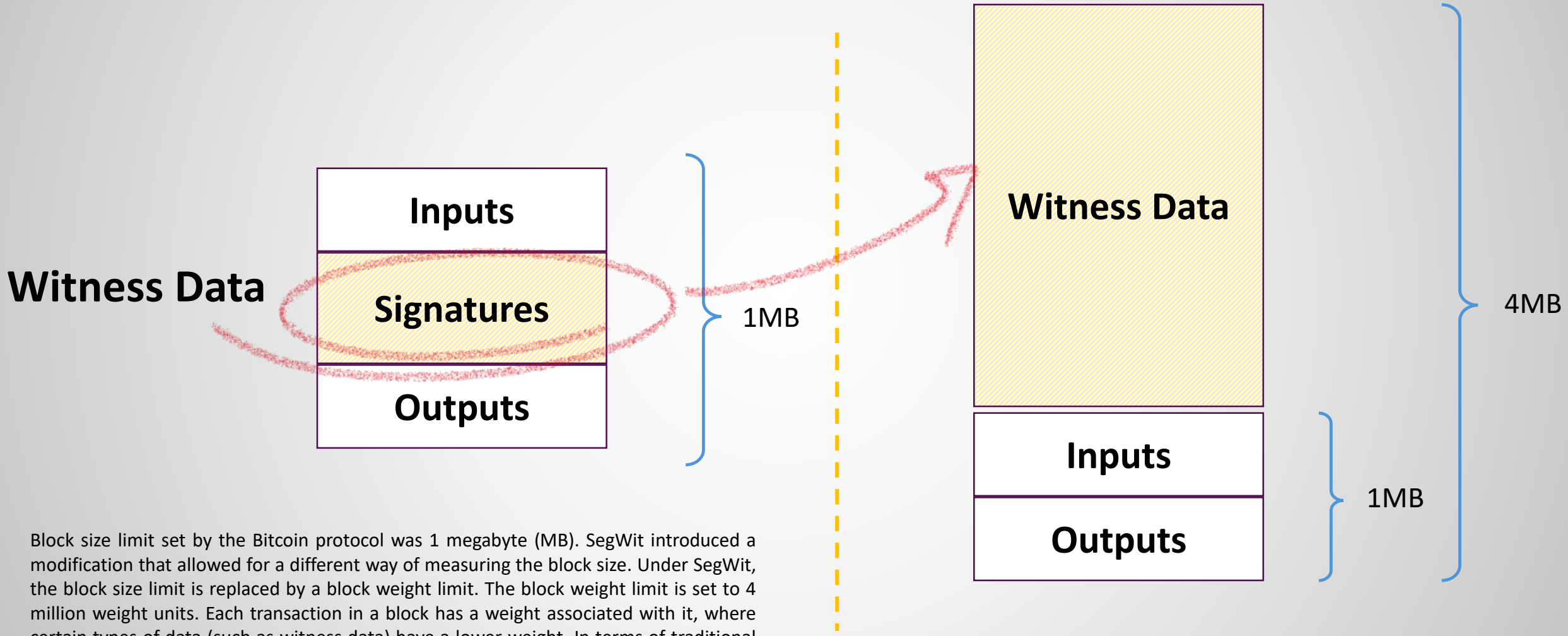
- Segwit was an upgrade made to Bitcoin in the so called Bitcoin Improvement Proposal 9 (BIP-9).
- It was implemented as a soft fork on Aug. 1, 2017.
- The term witness mainly refers to the transaction digital signature. However, it can refer to the solution to a cryptographic puzzle in a broader sense too.
  - The witness satisfies a condition placed on a transaction output and unlocks it for spending.

Traditional Block vs Segwit Block



(Image from exodus.com)

Traditional Block vs Segwit Block



Block size limit set by the Bitcoin protocol was 1 megabyte (MB). SegWit introduced a modification that allowed for a different way of measuring the block size. Under SegWit, the block size limit is replaced by a block weight limit. The block weight limit is set to 4 million weight units. Each transaction in a block has a weight associated with it, where certain types of data (such as witness data) have a lower weight. In terms of traditional block size, the block size limit for SegWit blocks is technically up to ~4 MB. However, because the weight of witness data is discounted, the effective increase in transaction capacity is around 1.7 to 2 MB.

Some Remarks on SegWit (BIP-9)

- Witness data range from 60% to 70% the transaction size.
  - Moving the witness part to a block extension can free up some space for more TXs in the 1MB quota.
    → Theoretically, more TPS and better scalability.
      - Have you heard that Bitcoin TPS is around 7? Seems that this is the number after the upgrade

- Witness section is discounted in the new block. Old network nodes can still embed the whole TX in the 1MB part, but miners demand higher commissions for that part.
  - It seems that it is more expensive to follow the old rules.

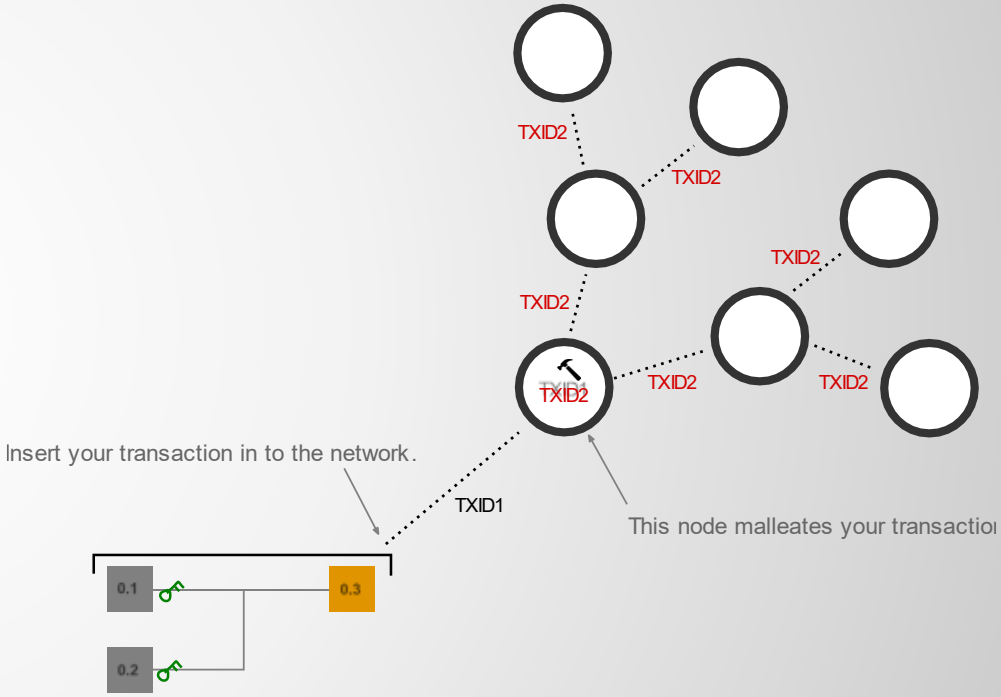
- Segwit signatures include the amount referenced by each input in the hash value (which is signed). Previously, the amount must have been fetched from the input transactions. Since the amount is part of the commitment hash now, offline devices do not need the previous TXs.

- The TX ID cannot be manipulated after the BIP-9 upgrade.
  → TXs are not malleable anymore

Transaction Malleability

Prior to Segwit, **TXID of a transaction could be changed by altering the unlocking code** in the transaction.

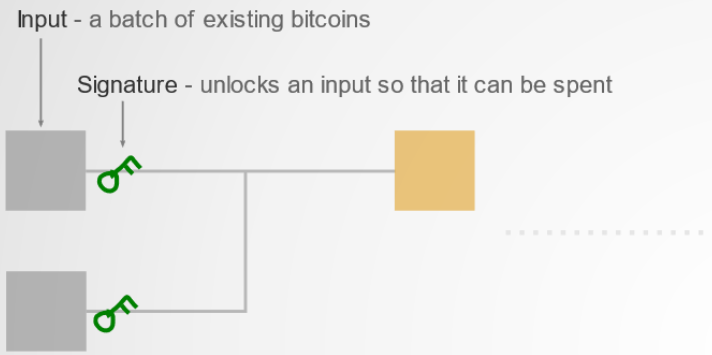
- E.g. by modifying the signature field without changing its value.
- This meant that when you sent your transaction to the network, any node had the ability to change the the TXID before passing it on.
- If the unlocking code is no longer part of the TXID, then no node will have the ability to change the TXID of your transaction.

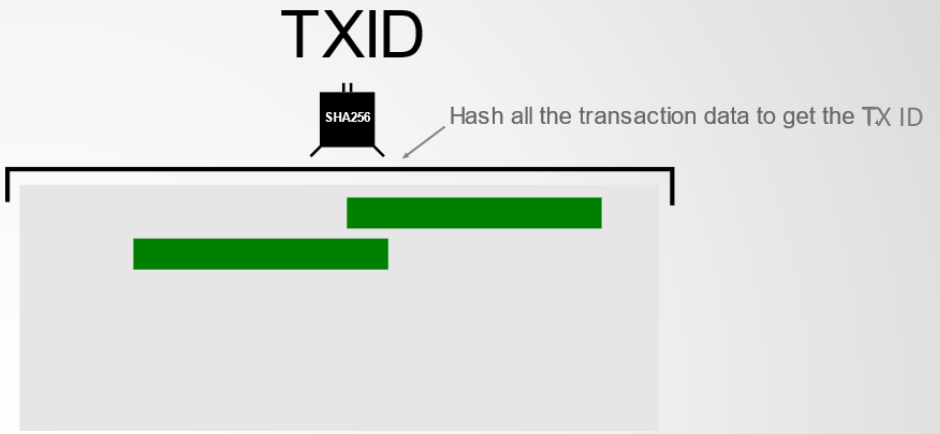


(learnmeabitcoin.com)

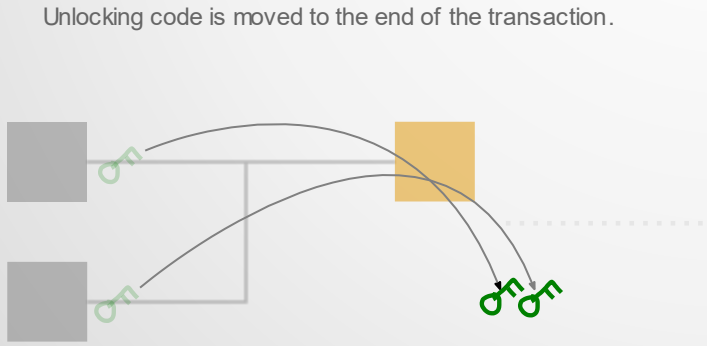
How Segwit Prevents Transaction Malleability

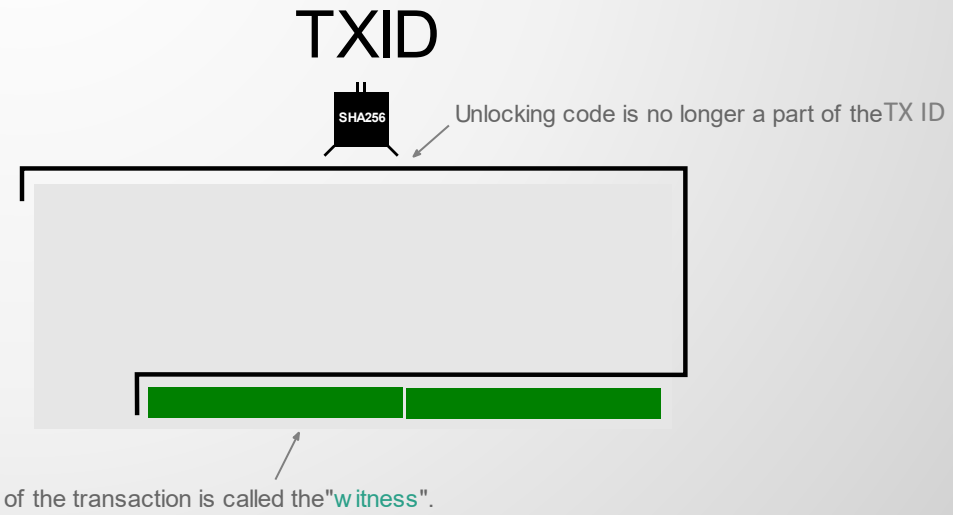
Non-Segregated Witness





Segregated Witness





(learnmeabitcoin.com)

P2WPKH & P2WSH

Pay-to-Witness-Public-Key-Hash (P2WPKH) is similar to P2PKH. You lock the transactions to a witness to the hash of the recipient's public key. The rightful recipient with the correct witness can unlock it under the Segwit framework.

Pay-to-Witness-Script-Hash (P2WSH) is similar to P2SH. You lock the transactions to a witness to the hash of a script. The rightful recipient with the correct witness can unlock it under the Segwit framework..

Segwit vs non-Segwit TXs

non-Segwit


```
{
  "txid": "87ae1a2fad2d8afe8160c5a7f15a64acbeead25cb8b32918facc1ef1cc8498a5",
  "size": 225,
  "version": 1,
  "locktime": 0,
  "fee": 11300,
  "inputs": [
    {
      "coinbase": false,
      "txid": "0f6731e51dc2313f67d8aa36f3db6872726798ebed7f6e859a6773b733cd6608",
      "output": 11,
      "sigscript":
"4730440220647cfc78c9b8c6c2d0641bc18940ec144292719a2c13dc85cf15c01c2c506a1d02201de777c6092f2115e50f9330c5c34
b2ac8991ad66789e90347c0de1996b06a5a0121039cb55f00dff5fd8426b4350a284a616a06d74382b9e6cc9af45c8b1aaafd5aad",
      "sequence": 4294967295,
      "pkscript": "76a914e46e07e579f2da2f62c33c960782baec8a1dbfa588ac",
      "value": 1195696,
      "address": "1MpppEwNAbMhizci9EHRcKYZZp8EBgm5L",
      "witness": []
    }
  ],
  "outputs": [
    {
      "address": "1M27g1g7yhL9zu8CgTcC1k2Vac4uRhS23A",
      "pkscript": "76a914db98806c7a80617d08dacec619026626065ae87b88ac",
      "value": 3716,
      "spent": true,
```


Segwit


```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
"3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed
6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpwgkqrsd7hnfx7v6w0456vr8077r",
```


Segwit addresses start with “bc1”.

What Comes Next …

- We learned about SegWit and BIP-9 soft fork.
- We saw how this improvement increased the Bitcoin performance and removed the TX malleability threat.
- We explain Bitcoin's Lightning Network in the next module, which is another solution proposed for Bitcoin scalability.

See you in the next module …