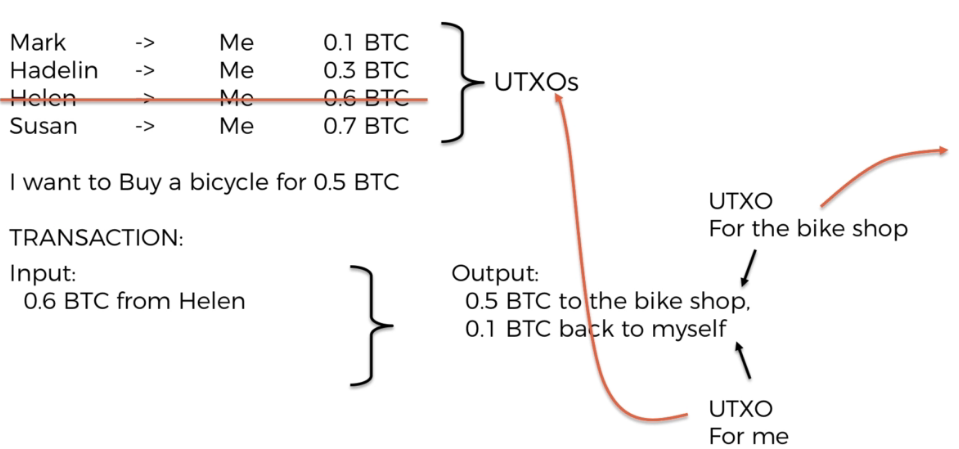
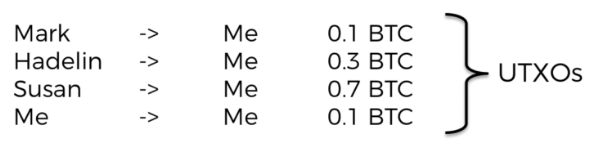
***Transactions and UTXOs (unspent transaction outputs):***



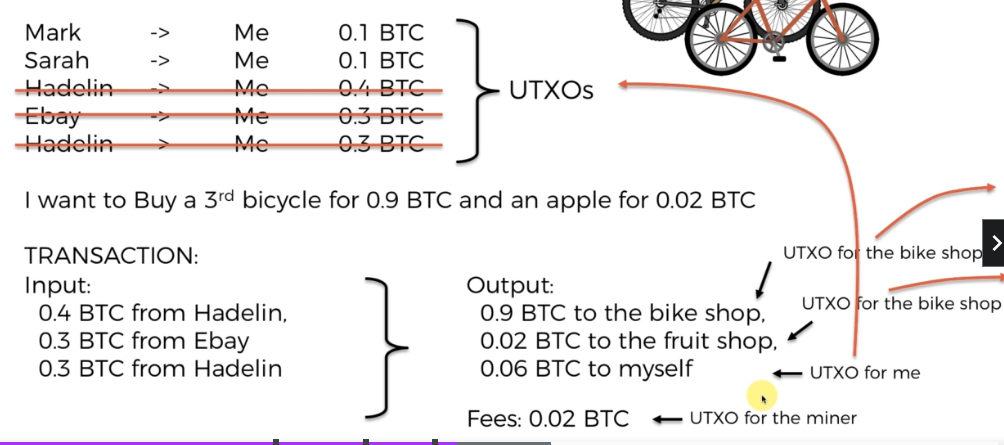
The rule is that there cannot be any unused outputs => Anything that goes into input, the full amount has to go into the output.

New UTXOs will be added



How the fees are generated:

Everything that you don’t account for will become a fee for that block.

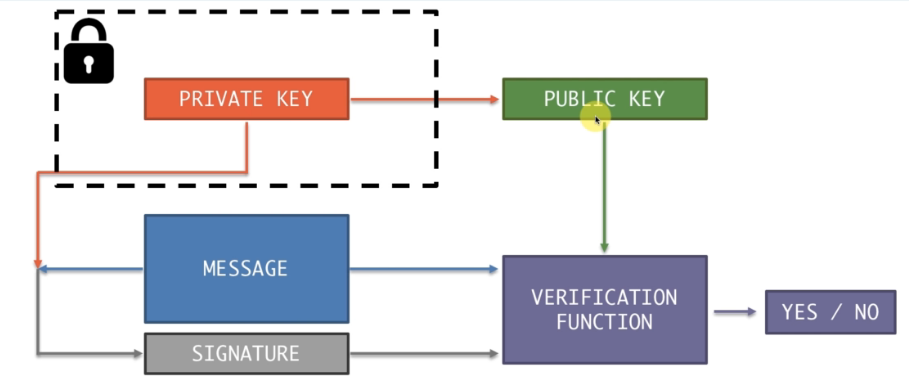


***How Wallets Work?***

After you made all of your transactions, the wallet will go through the whole blockchain and check what transactions have ‘you’ as destination and sum up all those UTXO transactions.



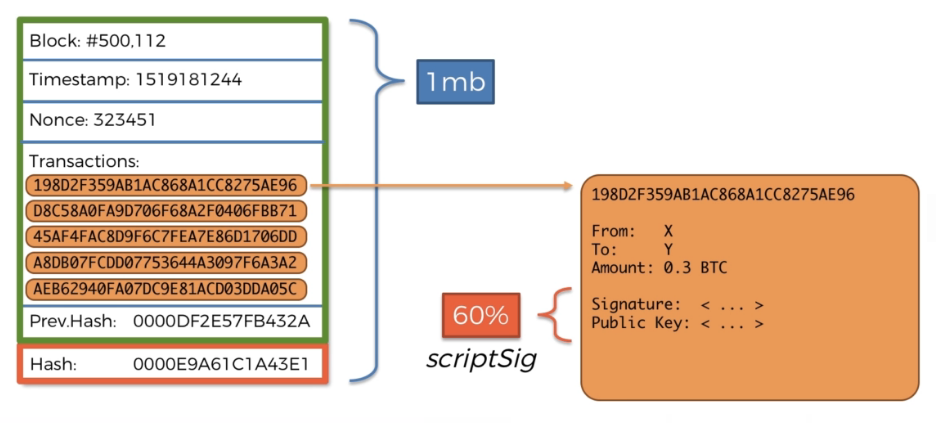
***Signatures: Private & Public Keys***



Private key is combined with the message and together they generate a signature. So the private key is used to sign the message. The transaction will travel with the signature. To verify that someone signed this signature (or someone who made the transaction), we use the public key. There is a verification function that takes 3 parameters: public key, message, signature and return a yes/no. Basically, they will use the public key to access the signature to confirm/deny that the transaction was made by that private key or technically speaking, they will check that is the signature created by the same private key which issued this public key.

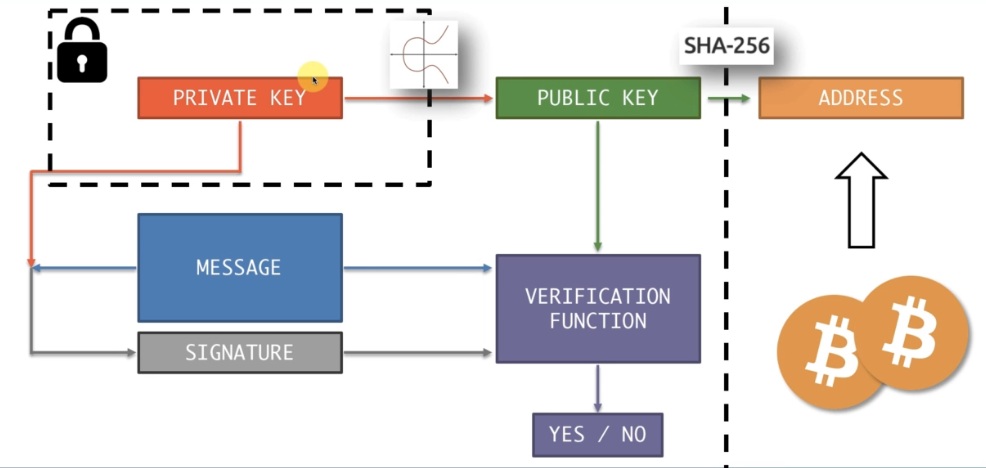
***Segregated Witness:***

Being a massive number, signature and public key (this combination is called scriptSig) have taken about 60% of the transaction size. And yet they are not the main purpose of the transaction. So the solution proposed was to take this part of the transaction and send its own through messaging service and on the network. So it will still be linked to each block and each transaction, but it will go through the network separately.



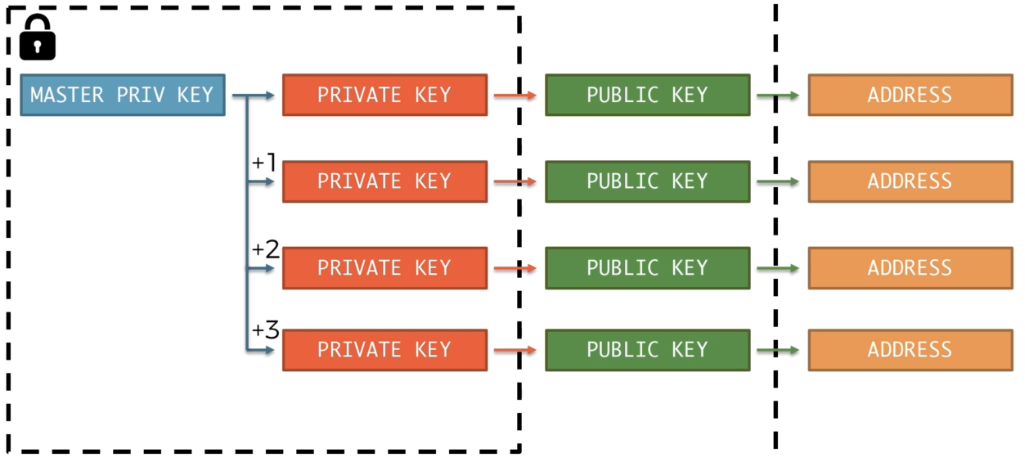
***Public Key vs Bitcoin Address:***

Address is generated by deriving SHA256 on public key. The reason we should have it is to have another layer of privacy. When receive Bitcoin, we should give Address.



***Hierarchically Deterministic (HD) Wallets:***

By using 1 private key, people could track how your public key and address behave. Like they could traverse the whole blockchain and see who you send and receive money from. Then they have pattern and it is a big concern. Therefore we have a master private key that could generate private key for each of our purposes. +1 to the master private key to generate a new private key.



The master private key is the 12 words (mnemonic) that the wallet provider will prompt you to write down a paper.