Transaction: Creation, Verification & Validation

Table of Content

In the dynamic realm of blockchain technology, the initial steps of transaction broadcasting and subsequent validation stand as the foundational pillars upon which the entire network's integrity and functionality rely. These primary stages serve a pivotal role in ensuring the secure, transparent, and reliable execution of transactions within a decentralized system.

The need for meticulous transaction broadcasting emerges from the decentralized nature of blockchain networks. Transactions, the heartbeat of any blockchain, necessitate seamless propagation across the distributed network. This dissemination process, facilitated by transaction broadcasting, fosters inclusivity by ensuring that every participating node possesses a record of the transaction. It initiates the journey of a transaction, from its inception by a user to its verification and eventual inclusion in the blockchain ledger. Without this widespread dissemination, the network's consensus mechanism would lack the requisite information to validate the transaction's authenticity and legitimacy.

Following this dissemination, the subsequent step of transaction validation emerges as the gatekeeper to the blockchain's sanctity. Validation involves a meticulous series of checks and verifications, encompassing digital signature scrutiny, fund availability assessment, and adherence to predefined consensus rules. Its significance lies in upholding the network's trust and security by filtering out invalid or malicious transactions. This step acts as a safeguard, ensuring that only legitimate and compliant transactions advance towards inclusion in the blockchain. Consequently, validation lays the groundwork for consensus mechanisms to operate effectively, as nodes collaboratively confirm the transaction's validity based on these pre-established criteria. Without this stringent validation, the blockchain's integrity would be susceptible to compromise, undermining its core principles of transparency and immutability.

Here is a detailed explanation of how this will happen:

1. **Transaction Broadcasting:**

- **Transaction Creation:** A user generates a transaction by specifying the recipient's address, the amount to be transferred, and potentially other necessary data (such as smart contract function calls in some blockchains).
- **Transaction Propagation:** The transaction is transmitted to the connected nodes in the network. This dissemination can happen through a gossip protocol, where nodes broadcast the transaction to their peers.

  Example: Imagine Alice wants to send 5 units of a cryptocurrency (let's call it "ABC coin") to Bob. To initiate this transaction:

Alice creates a transaction specifying Bob's address as the recipient, the amount (5 ABC coins), and signs the transaction with her private key.

This transaction is then broadcasted across the decentralized blockchain network. Every node in the network receives this transaction.

For instance, Node A, Node B, and Node C in the blockchain network receive the transaction initiated by Alice.

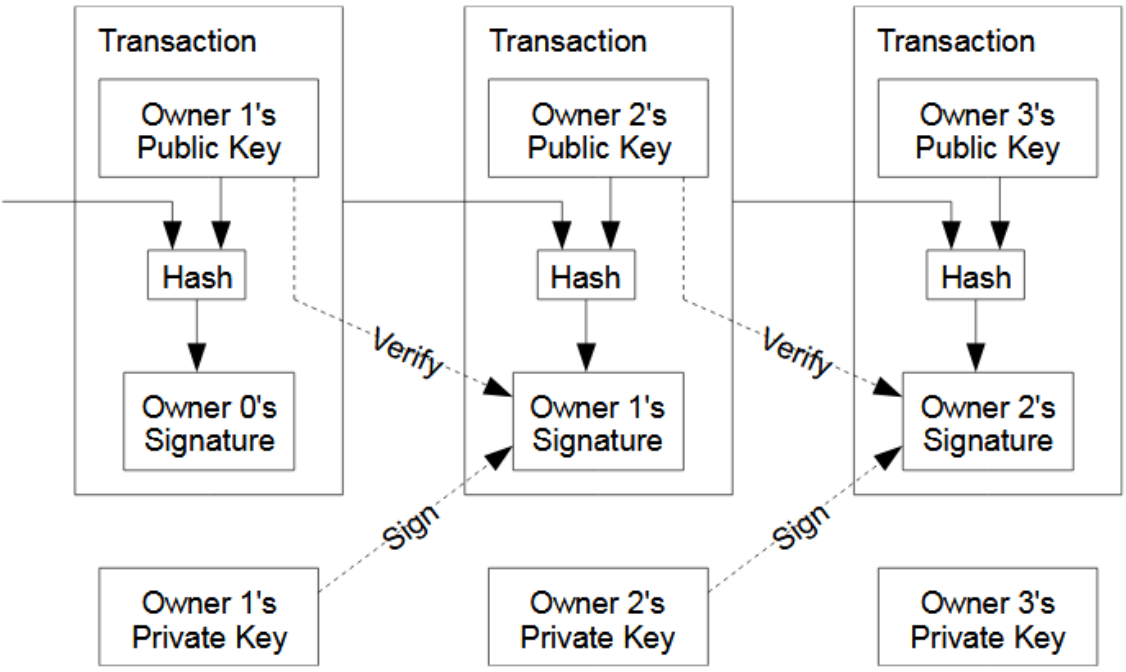
2. Transaction Validation:

Upon receiving Alice's transaction, each node in the network verifies its authenticity and validity before considering its inclusion in the next block. The validation process includes several checks:

- **Digital Signature Verification:** Nodes receive the transaction and verify the digital signature using the sender's public key. This process confirms the transaction's authenticity and ensures it was indeed initiated by the owner of the private key.

  Each node confirms that Alice's digital signature matches her public key and ensures the signature is valid, verifying that Alice is the actual sender.

What is Digital Signature?



Digital Signature are done using public and private key, so what are they

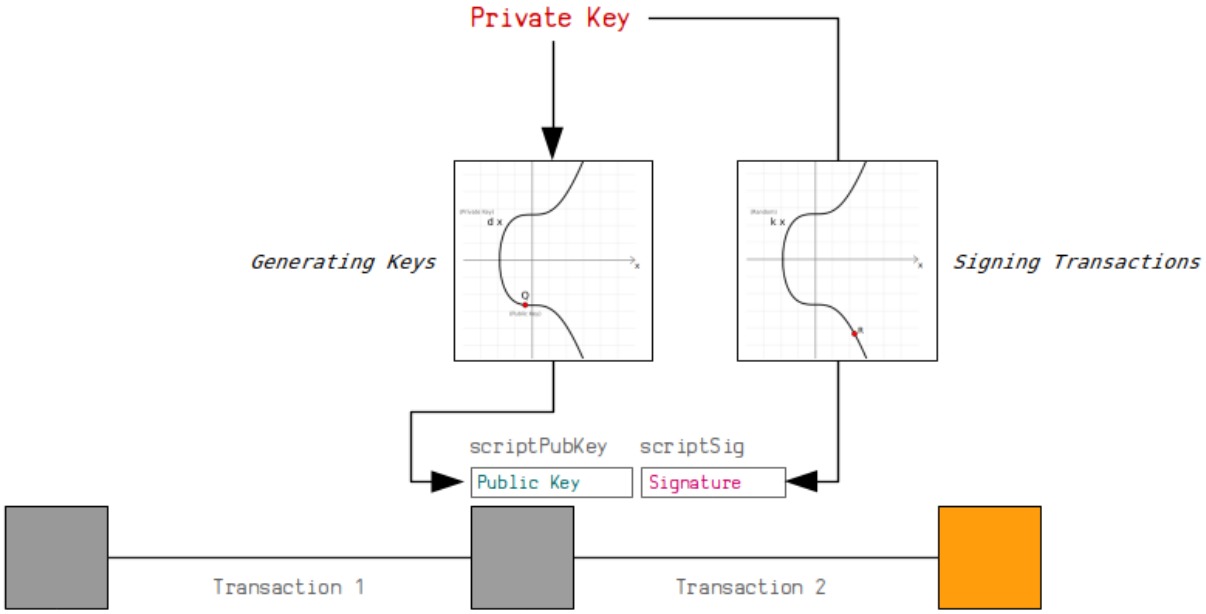
ECDSA

Bitcoin uses a digital signature system called ECDSA to control the ownership of bitcoins.

In short, a digital signature system allows you to generate your own private/public key pair, and use the private key to generate digital signatures that proves you are the owner of the public key without having to reveal the private key.

This system is used in Bitcoin to allow people to receive and send bitcoins. Anyone can generate their own pair of keys, and then anyone can send (or "lock") bitcoins to your public key. Nobody can steal these bitcoins, because only the person with the correct private key for this public key is able to generate valid signatures to "unlock" the bitcoins and send them to someone else.

The ability to create digital signatures has been around since the 1970s thanks to the invention of RSA. In 1994, DSA was released as the standard for digital signature systems. ECDSA is just an implementation of DSA using *elliptic curve* cryptography, as the mathematics of elliptic curves allow for more efficient signature creation and verification.



After this fund availability is checked.

- **Funds Availability Check:**

Nodes check the sender's account balance or UTXOs (Unspent Transaction Outputs) to ensure they have sufficient funds for the transaction.

Nodes check Alice's address in the ledger to confirm she has at least 5 ABC coins available to send. If she has insufficient funds, the transaction will be rejected.

How is fund availability checked?

UTXO

In bitcoin, the transaction lives until it has been executed till the time another transaction is done out of that UTXO. UTXO stands for Unspent Transaction Output.

It is the amount of digital currency someone has left remaining after executing a transaction.
When a transaction is completed, the unspent output is deposited back into the database as input which can be used later for another transaction.
The UTXO model does not incorporate wallets at the protocol level. It is based on individual transactions that are grouped in blocks. The UTXO model is a design common to many cryptocurrencies, most notably Bitcoin.
Cryptocurrencies that use the UTXO model do not use accounts or balances. Instead, UTXOs are transferred between users much like physical cash.
Each transaction in the UTXO model can transition the system to a new state, but transitioning to a new state with each transaction is infeasible.
The network participants must stay in sync with the current state.

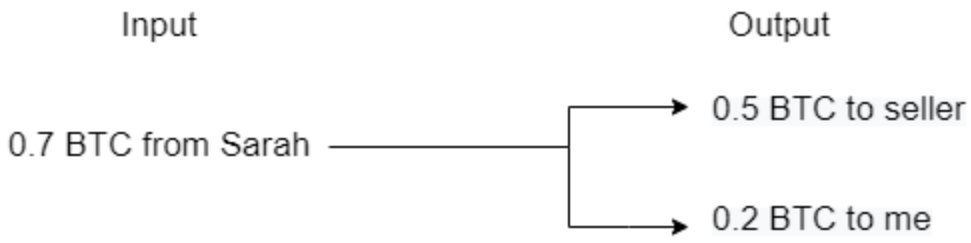
Example:
Suppose the following bitcoins are received from the transactions. Each one of these transactions is a UTXO.

John -> Me 0.1 BTC

Sarah -> Me 0.7 BTC

Sam -> Me 0.4 BTC

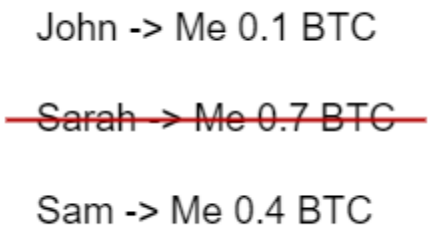
1. Now I want to buy a car that costs 0.5 BTC.
2. In order to transfer 0.5 BTC, there is a need to choose one or multiple transactions as input.
3. This is why, a transaction in bitcoin is different from banks, in the case of banks, one would have entered an amount of 0.5 BTC, pressed transfer and it would have gone to the seller, but this is not the case in bitcoin, here there is a need to choose one or more UTXOs as the input.
4. In the case of cryptocurrency, there is no such thing as an amount lying in your account.
5. Let's choose 0.7 BTC from Sarah as input to purchase a car.



6. In the case of UTXO, the input amount can't be left unspent, one can't say that do nothing with the remaining 0.2 BTC.
7. The remaining 0.2 BTC, has to be used in one of the following 3 ways-
8. Send the remaining amount back to your account, as we did in the above image.
9. Use the remaining amount as the transaction fee. Remember, that there should be some transaction fee otherwise no miner will add your transaction to block, and it will remain unconfirmed.

10. Send the remaining amount to someone else.
11. Now that 0.5 BTC has been sent to the seller but no fee has been added, the transaction didn't get confirmed, and after 72 hours, 0.7 BTC will be refunded back.
12. So, in order to send money to the seller, let's put those 0.2 BTC as fees for this transaction.
13. In order to provide a transaction fee, nothing needs to be mentioned, if you don't send the remaining amount to anyone, it is assumed a transaction fee.

14. Now that the transaction fee has been added, a miner included this transaction in the block and subsequently got 0.2 BTC as the transaction fee.
15. Let's have a look at our original UTXOs again.



16. The UTXO from Sarah is no longer there, the UTXO only lived till another transaction was not done from it, but now it has been used in another transaction, i.e. to purchase the car.
17. Transaction is stored inside a block, also it is one of four factors that changes the hash of a block. This means if a miner chooses a different transaction keeping the other 4 factors the same, the hash will be different.
18. The factors that determine the hash of a block

- **Consensus Rule Validation:** The transaction is examined against consensus rules. For instance, nodes ensure that the transaction isn't attempting double spending (sending the same funds to multiple recipients) and adheres to the protocol's format and rules.

In our example, Node A, Node B, and Node C independently perform these validations upon receiving Alice's transaction. Each node ensures the digital signature matches, checks Alice's account balance, and validates the transaction against the consensus rules.

If all checks pass successfully, the transaction is considered valid and ready to be included in a block. Nodes will then add this validated transaction to their mempool, awaiting selection by miners or validators to become part of the next block in the blockchain.

3. **Propagation and Pooling:**

- **Mempool Inclusion:** Validated transactions are added to the mempool of each node. The mempool acts as a temporary holding area for pending transactions waiting to be included in a block.

- **Mempool Management:** Transactions might stay in the mempool for varying durations based on factors like transaction fees, priority, or network congestion.

Post this Block Creation and Mining happens