Comparison of Cryptocurrencies Transactions

Bitcoin, and other cryptocurrencies, exist due to its blockchain, which is a non-centralised distributed ledger. The blockchain is made of blocks that are connected to one another. The blocks are the basic structure where the transactions are stored. We can then say that a transaction is the basic unit of the blockchain, in the same way an amino acid is the basic unit of a protein, or a nucleotide is the basic structure of the DNA. Therefore, to understand blockchains and Cryptocurrencies, we need to start by understanding how transactions work.

A transaction is a form of moving money from one entity to another, which we can call them "sender" and "receiver". The sender takes money **out**, hence she generates an "output", and the receiver brings money **in**, hence she generates an input. The output and the input are the basic structures of a transaction.

In Bitcoin, the sender generates an output, which must include: the index, the amount in Satoshis, which is the smallest unit of bitcoin (10^8 satoshis =1BTC), and the ScriptPubKey, which states the conditions to use the money from this output. The ScriptPubKey is composed of a script of few commands and the receiver address in the middle. This address is the hashed value of the receiver public key. Once this is generated, this can be called, UTXO (Unspent Transaction Output).

The input, which is generated by the receiver, has two main components: The first one is a pointer to reference the UTXO by its transaction hash and its index, and the second component is the SigScript. The SigScript is composed of the public key and a signature. These are needed to address the conditions generated in the ScriptPubKey and this way, the receiver can have access to the money in the output.

The verification of the transaction is done by joining the ScriptPubKey with the SigScript and running them together. The basic data structure in bitcoin is the stack where data is added and removed similar to a stack of bricks, last in, first out. Similarly, the operations are carried out only on the last element(s).

First, the SigScript is run, where the signature and the public key are added into the stack. In the second step, the ScriptPubKey is run. This one, instructs the public key (the last element in the stack) to be duplicated, then to be hashed with SHA-256, then, the address (which is the hash of the receiver public key) is added to the stack. In the next step, it runs a verification if the last two elements are equal, which are the hash of the public key, given by the receiver, and the address, which was given by the sender, that should equal the hash of the receiver public key. If the two are equal, as they should, the two are removed from the stack. If not, the program raises an error and the transaction is considered invalid. Finally, the last command checks the public key against the signature, which verifies that the receiver has control of the public key.

Until the receiver generates a new output using the money from this transaction, the transaction will not be verified, and the money will still be considered a UTXO.

From this, we can understand that Bitcoin transactions do not store any personal information about the sender and the receiver, neither their bitcoin balance. They only store addresses and public keys, however, a single person can generate multiple public keys which belong to her. In addition, all the money a bitcoin user owns is stored in different UTXOs in the blockchain which she can get redeemed. Generally, these are managed in the so-called "wallet".

It is important to remark that Bitcoin transactions are not free. For them to be part of a new block in the blockchain, a small fee needs to be paid in each transaction to the miner, who does the job of including it in the block. The fee is an unexplicit amount which is the difference between the sum of inputs and the sum of outputs. It should be relatively high to be considered relevant by the miner but should be small enough for the sender to be worth creating the transaction with one or more specific UTXOs.

Bitcoin is not very flexible, as it is not Turing-Complete and does not allow loops. Its main aim is to transfer money from one entity to another. Bitcoin is the first developed cryptocurrency while Ethereum is the second, hence some Ethereum properties came to “improve” or upgrade Bitcoin functionality, giving the blockchain more flexibility.

Ethereum works with a Turing complete programming language, and this allows the users, not only to transfer money but to produce smart contracts and applications which can run in the system.

Ethereum transactions are different than those in Bitcoin. First of all, we can find that users have accounts, which have a specific state, the amount of Ether, a nonce and the storage. There are two types of Ethereum accounts, Externally Owned Accounts (EOA) and Smart Contracts. Ethereum transaction has the account addresses of the sender and the receiver. Hence, Bitcoin has more privacy than Ethereum. Another big difference is in the fee that is payable to the miner. Ethereum transactions have two explicit values that correspond to the fee, the Gas limit, which is the maximum amount of gas the sender is willing to pay, and the Gas price, the maximum amount of Ether the sender is willing to pay for each Gas unit. In addition, Ethereum transactions have a “data” variable to add extra information which is added or modified in the account storage. In addition, in Ethereum transactions, the sender signs, with her private key, the transactions. This adds extra security to the transaction and a more-straight forward verification process. The Ethereum transactions could be verified by any node in the network with simple programming functions using the sender public key, the transaction signature, and data. As the nonce of the account changes after every transaction, it is not possible to replicate a transaction because the signature includes the nonce of the account when the transaction was done.

To summarise, Ethereum and Bitcoin transactions are both secure, however, it is easier to verify Ethereum transactions. Ethereum has more flexibility and has more functionalities than bitcoin as it is possible to generate smart contracts and run specific programs. Moreover, in Ethereum it is easier to control the fee the sender is willing to pay for a transaction. On the other side, Bitcoin has stronger data privacy.

References

Antonopoulos, AM 2017, Mastering Bitcoin : Programming the Open Blockchain, O'Reilly Media, Incorporated, Sebastopol.

Chowdhury, N 2019, Inside Blockchain, Bitcoin, and Cryptocurrencies, Auerbach Publishers, Incorporated, Milton.