Unspent Transaction Outputs(UTXO)

Bitcoin, and many protocols based on it, store data about transactions and user balances in the form of unspent transaction outputs, which are a list of “unspent” Bitcoin amounts that have been sent to a user, but have not yet been sent from him/her. The sum of these outputs is the user’s total balance. On the blockchain, they appear to be a collection of Bitcoin amounts on different addresses, and the role of a wallet is to identify which addresses the user has keys to. Individual Bitcoin are easy to track because they are signed from one person to another. A transaction is valid if one can prove ownership over the actual Bitcoin s/he is trying to send.

This is in contrast to Ethereum’s account model, which stores information about the entire balance associated with a user’s account. Other users send tokens to and from their own accounts. Individual ETH are more difficult to track because they are added and subtracted to user balances. A transaction is valid if one can prove ownership over the account and the account’s balance is high enough to support it.

The UTXO system is like a digital recreation of a cash economy. For example, Alice gives Bob 1 BTC , and the system now recognizes that there is 1 BTC signed to Bob that he has not yet given to anyone else. If Bob already had 1 BTC, then his balance on the blockchain would be 1 BTC + 1 BTC. Bob’s Bitcoin balance is the sum of all Bitcoin signed to him, similar to how all the fiat cash in Bob’s leather wallet is the sum of all fiat cash given to him. If he wants to combine his two separate BTC, he must do so in another transaction, much like he needs to do if combining two $5 bills into a $10 bill.

In contrast, the account model is like a bank account that automatically maintains user balances, similar to how a bank maintains a single balance amidst spending and receiving funds. When Alice gives Bob 1 ETH, the system now recognizes that Bob’s balance has gone up by 1 ETH and Alice’s has gone down. If Bob already had 1 ETH, then his balance on the blockchain would be 2 ETH. He does not need another exchange to combine them in his account.