Reminder: The Simple UTxO-Model

The Simple UTxO-Model

- UTxO is an acronym for Unspent Transaction Output.

The Simple UTxO-Model

- UTxO is an acronym for Unspent Transaction Output.
- As in the account-based model (employed for example by Ethereum), the UTxO-model uses (hashes of) public keys as addresses.

The Simple UTxO-Model

- UTxO is an acronym for Unspent Transaction Output.
- As in the account-based model (employed for example by Ethereum), the UTxO-model uses (hashes of) public keys as addresses.
- A transaction has UTxOs as inputs and one or more outputs.

The Simple UTxO-Model

- UTxO is an acronym for Unspent Transaction Output.
- As in the account-based model (employed for example by Ethereum), the UTxO-model uses (hashes of) public keys as addresses.
- A transaction has UTxOs as inputs and one or more outputs.
- Transactions are authorized by the digital signatures of the owners of the inputs.

The Simple UTxO-Model

- UTxO is an acronym for Unspent Transaction Output.
- As in the account-based model (employed for example by Ethereum), the UTxO-model uses (hashes of) public keys as addresses.
- A transaction has UTxOs as inputs and one or more outputs.
- Transactions are authorized by the digital signatures of the owners of the inputs.
- Transactions with several senders and/or receivers are possible.

The Simple UTxO-Model

- UTxO is an acronym for Unspent Transaction Output.
- As in the account-based model (employed for example by Ethereum), the UTxO-model uses (hashes of) public keys as addresses.
- A transaction has UTxOs as inputs and one or more outputs.
- Transactions are authorized by the digital signatures of the owners of the inputs.
- Transactions with several senders and/or receivers are possible.
- The state of the blockchain is determined by the set of all UTxOs.

The UTxO-Model (continued)

- For each transaction, the sum of all inputs (plus transaction fees) must equal the sum of all outputs.

The UTxO-Model (continued)

- For each transaction, the sum of all inputs (plus transaction fees) must equal the sum of all outputs.
- Each transaction completely spends all its inputs. If the sum of inputs is too large, an output has to be created for the change.

The UTxO-Model (continued)

- For each transaction, the sum of all inputs (plus transaction fees) must equal the sum of all outputs.
- Each transaction completely spends all its inputs. If the sum of inputs is too large, an output has to be created for the change.
- A transaction consists of:
  - A set of inputs (UTxOs).

The UTxO-Model (continued)

- For each transaction, the sum of all inputs (plus transaction fees) must equal the sum of all outputs.
- Each transaction completely spends all its inputs. If the sum of inputs is too large, an output has to be created for the change.
- A transaction consists of:
  - A set of inputs (UTxOs).
  - An ordered list of outputs, where each output has an address and a value.

The UTxO-Model (continued)

- For each transaction, the sum of all inputs (plus transaction fees) must equal the sum of all outputs.
- Each transaction completely spends all its inputs. If the sum of inputs is too large, an output has to be created for the change.
- A transaction consists of:
  - A set of inputs (UTxOs).
  - An ordered list of outputs, where each output has an address and a value.
  - A digital signature for each input.

Transaction Validity in the UTxO-Model

A transaction in the UTxO-model is valid if the following three conditions are satisfied:

Transaction Validity in the UTxO-Model

A transaction in the UTxO-model is valid if the following three conditions are satisfied:

- The transaction contains digital signature's belonging to the owners of the inputs.

Transaction Validity in the UTxO-Model

A transaction in the UTxO-model is valid if the following three conditions are satisfied:

- The transaction contains digital signature's belonging to the owners of the inputs.
- The sum of all input values (plus transaction fees) equals the sum of all outputs.

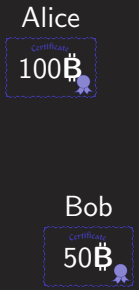
Transaction Validity in the UTxO-Model

A transaction in the UTxO-model is valid if the following three conditions are satisfied:

- The transaction contains digital signature's belonging to the owners of the inputs.
- The sum of all input values (plus transaction fees) equals the sum of all outputs.
- No output value is negative.

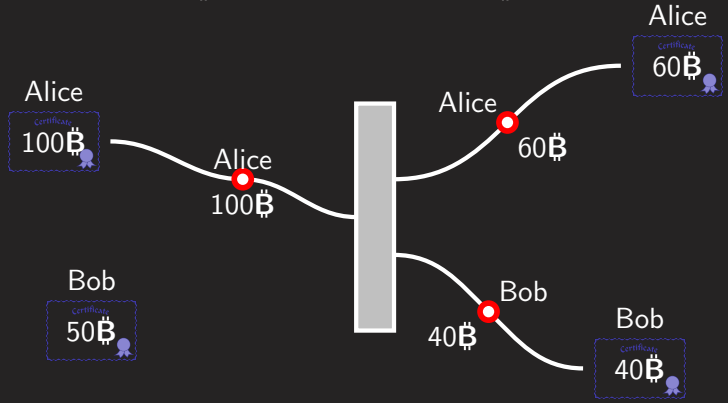
Example: A Simple Transaction

Alice holds 100 ฿ and wants to send 40 ฿ to Bob, who has 50 ฿.



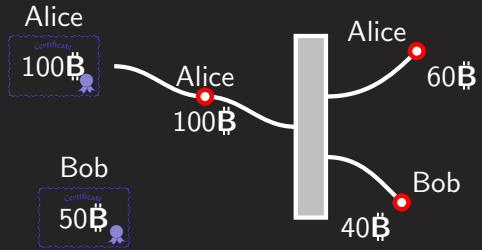
Example: A Simple Transaction

Alice holds 100 ₿ and wants to send 40 ₿ to Bob, who has 50 ₿.



Example: A More Complex Transaction

After sending 40 ₿ to Bob, Alice and Bob want to send 55 ₿ each to Charlie.



Example: A More Complex Transaction

After sending 40 ₿ to Bob, Alice and Bob want to send 55 ₿ each to Charlie.