Blockchain Council™

UTXO Model Vs Account Model

Transaction - UTXO Vs Account Model

- A transaction is an event that the user initiates to transfer funds on a blockchain. This transaction informs the network of the number of assets, the sender and the new owner.

- Transactions are batched together to create a block which is added to the blockchain. The system goes through a state transition with each new block.

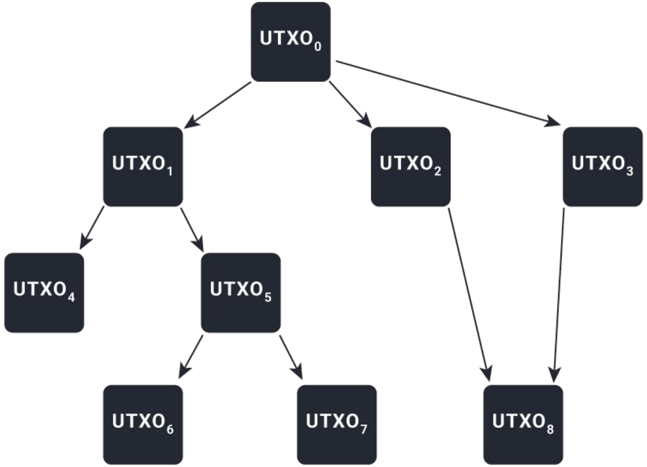
- The user interactions, mainly transactions, are broadcasted to the network, confirmed, and are recorded with each new block.

- When the system transitions to a new state, the balances of the transacting parties are updated.

UTXO Vs Account Model

Blockchain Council™

UTXO Model



Directed graph of assets(UTXOs) moving between users

Account Model

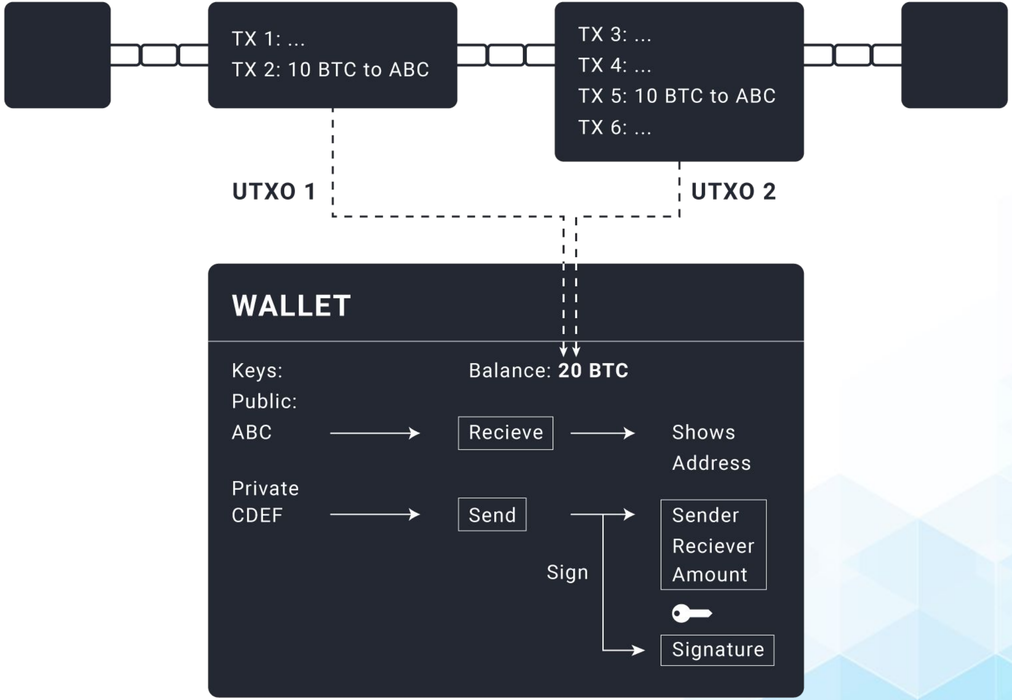
State n	Account A	Balance t_0
	↓	
State (n+1)	Account A Account B	Balance t_1 Balance t_1
	↓	
State (n+2)	Account A Account B	Balance t_2 Balance t_2
	↓	
State (n+3)	Account A Account B Account C	Balance t_3 Balance t_3 Balance t_3

Database of network states

UTXO Model

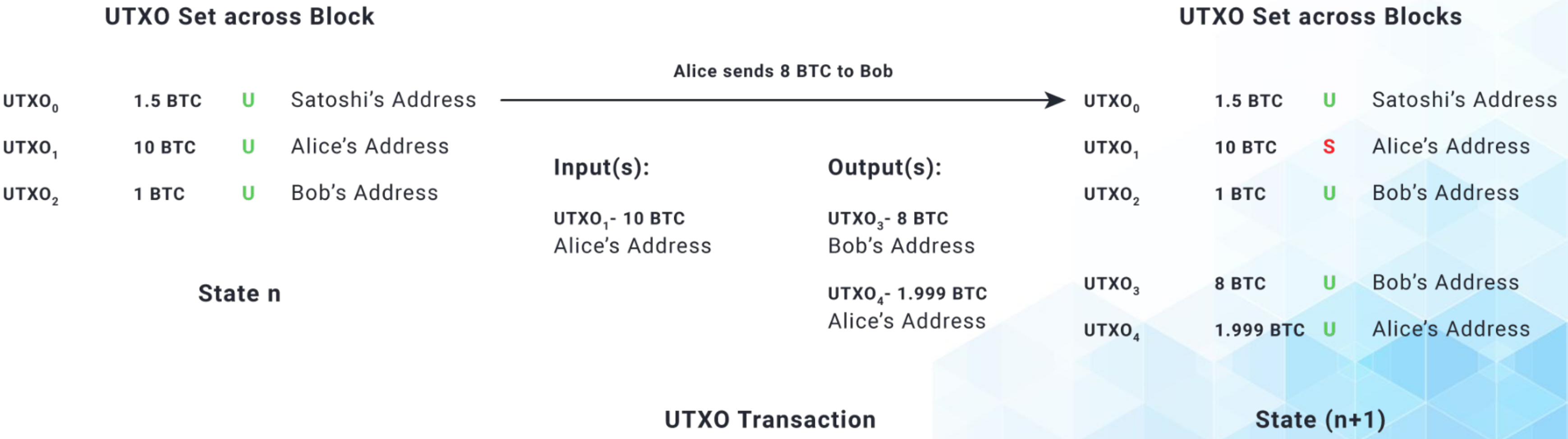
- At the protocol level, the UTXO model uses Individual transactions clustered into blocks to form the basis of the model.
- A user with 20 BTC may have control over a single UTXO worth 20 BTC or a collection of UTXOs worth 20 BTC.
- In the case of partial amount transfer, the difference between the UTXO size and the amount the user wants to transfer is transmitted as a change to a self-controlled address.
- Spending 15 BTC from a 20 BTC UTXO results in two outputs in the transaction: a 15 BTC output to the payee and a 5 BTC shift output to the original owner.

UTXO Model


TX 1: ...
TX 2: 10 BTC to ABC
TX 3: ...
TX 4: ...
TX 5: 10 BTC to ABC
TX 6: ...
UTXO 1
UTXO 2
WALLET
Keys:
Public:
ABC
Private
CDEF
Balance: 20 BTC
Recieve
Shows
Address
Send
Sign
Sender
Reciever
Amount
Signature

State Transitions in the UTXO Model

- In UTXO, each transaction represents a state change in the network, but doing so is difficult and unscalable.
- The blockchain uses blocks to batch transactions which represents any state transition in the system.



UTXO Set across Block

UTXO_0	1.5 BTC	U	Satoshi's Address
UTXO_1	10 BTC	U	Alice's Address
UTXO_2	1 BTC	U	Bob's Address

State n

Alice sends 8 BTC to Bob

Input(s):

UTXO_1- 10 BTC
Alice's Address

Output(s):

UTXO_3- 8 BTC
Bob's Address

UTXO_4- 1.999 BTC
Alice's Address

UTXO Transaction

UTXO Set across Blocks

UTXO_0	1.5 BTC	U	Satoshi's Address
UTXO_1	10 BTC	S	Alice's Address
UTXO_2	1 BTC	U	Bob's Address
UTXO_3	8 BTC	U	Bob's Address
UTXO_4	1.999 BTC	U	Alice's Address

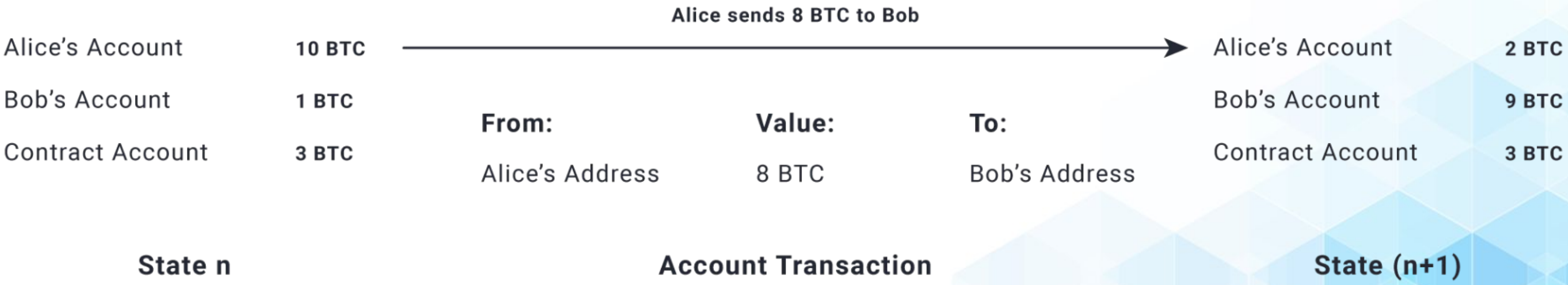
State (n+1)

Account based Model

- The account-based transaction model represents assets as a product of the account’s balance. Ethereum cryptocurrency uses this method in its native cryptocurrency.
- In the account-based paradigm, transaction are represented as decrement in the sender's account balance and increase in the receiver's account balance.
- Each transaction in the account model has a nonce tied to it to avoid double-spending attacks.
- In Ethereum, each account has public viewable nonce that is incremented by one with each outgoing transaction. This stops transfers from being sent to the network several times.

State Transitions in the Account Model

- In the account model, the transaction poses the same problem of continuous state change.
- To prevent this, the transactions are batched into blocks, with each block representing a state change in the blockchain.



Alice sends 8 BTC to Bob

Alice’s Account	**10 BTC**
Bob’s Account	**1 BTC**
Contract Account	**3 BTC**

State n

From:	**Value:**	**To:**
Alice’s Address	8 BTC	Bob’s Address

Account Transaction

Alice’s Account	**2 BTC**
Bob’s Account	**9 BTC**
Contract Account	**3 BTC**

State (n+1)

Blockchain Council™

THANK YOU!

Any Questions?

Visit

community.blockchain-council.org

Mail Us

hello@blockchain-council.org