Chapter 4

TRANSACTIONS AND TRANSACTION PROCESSING

TP. HCM 2022

OVERVIEW

- Transaction Input and Output Explanation
- Unspent Transaction Output
- Blockchain Design

Group discussion

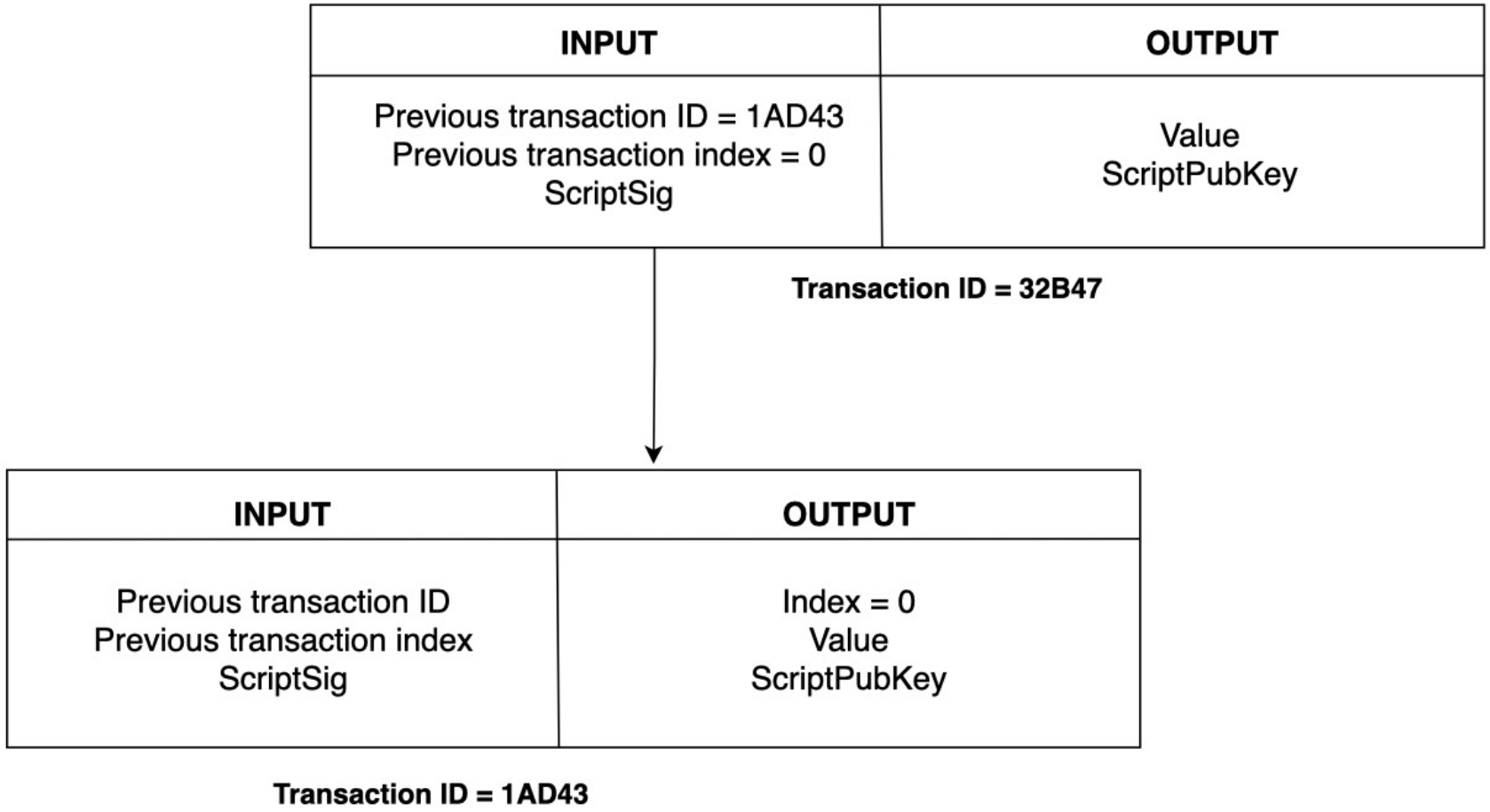
- What fileds included in the transaction format of a blockchain?
- Explain coinbase transaction?
- Unspent Transaction Output (UTXO) model vs Account-based model?
  - Discussion time: 30 minutes
  - Presentation: 5 minutes

TRANSACTION FORMAT

INPUT	OUTPUT
Previous transaction ID Previous transaction index ScriptSig	Value ScriptPubKey

- **Previous transaction ID**: the ID of the transaction in which that Bitcoin was created as output and assigned to the current owner.
- **Previous transaction index**: Every Bitcoin transaction can have multiple outputs (an array of outputs), and every output is identified by a unique index (index of the array). This index, along with the previous transaction ID, can be used to locate the transaction where that Bitcoin was created and to identify its real owner.
- **ScriptSig (script signature):**
  - Encodes the public key and the signature of the current owner of the Bitcoin (payer).
  - Format: <Digital signature of the payer>
    <Public key of the payer>

TRANSACTION FORMAT: input



Every input of a transaction is linked to an output of a previous transaction.

image source: https://www.educative.io

TRANSACTION FORMAT: output

INPUT	OUTPUT
Previous transaction ID Previous transaction index ScriptSig	Index = 0 Value ScriptPubKey
	Index = 1 Value ScriptPubKey
Previous transaction ID Previous transaction index ScriptSig	Index = 2 Value ScriptPubKey

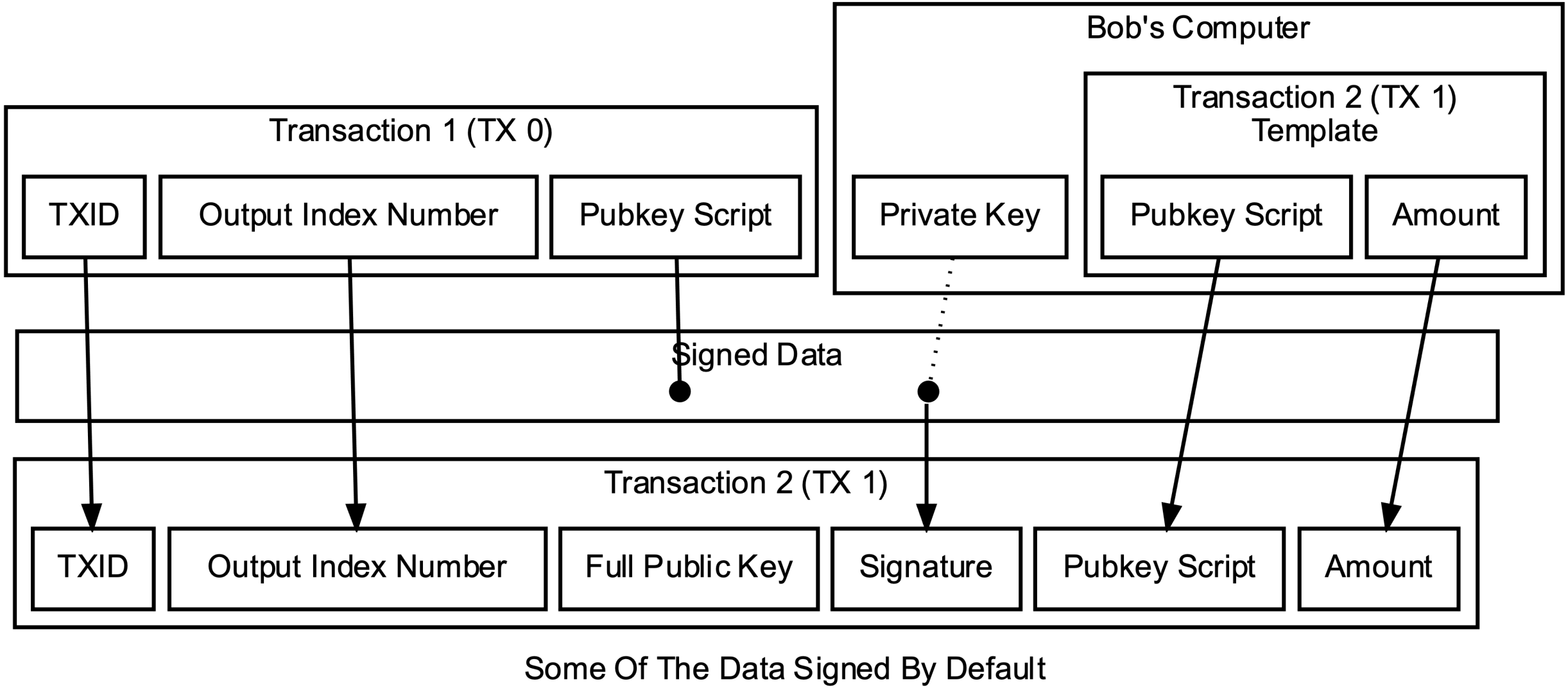
image source: https://www.educative.io

TRANSACTION FORMAT: output

- **Value:**
  - The number of Bitcoins being transferred to the payee.
  - The minimum value that a user can transfer is one satoshi
  - 10^8 satoshis = 1 Bitcoin
- **ScriptPubKey:** a sequence of instructions (like a function)
  - takes ScriptSig as input
  - returns true if a legitimate owner tries to unlock that Bitcoin.
  - otherwise, it returns false.
  - format of a ScriptPubKey:

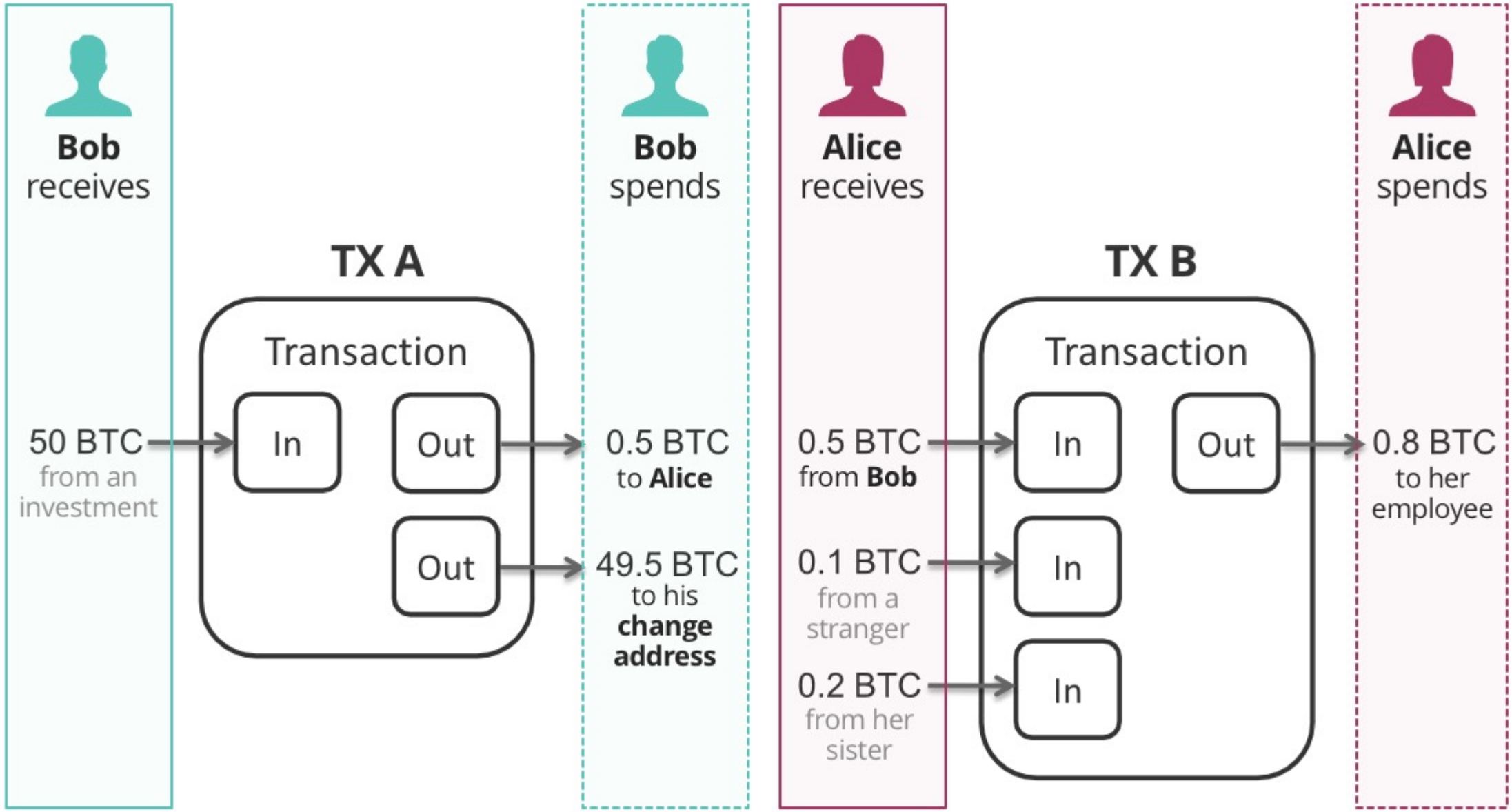
```
OP_DUP
OP_HASH160
<Hash(PubKey)>
OP_EQUAVERIFY
OP_CHECKSIG
```

TRANSACTION FORMAT



Some Of The Data Signed By Default

TRANSACTION FORMAT



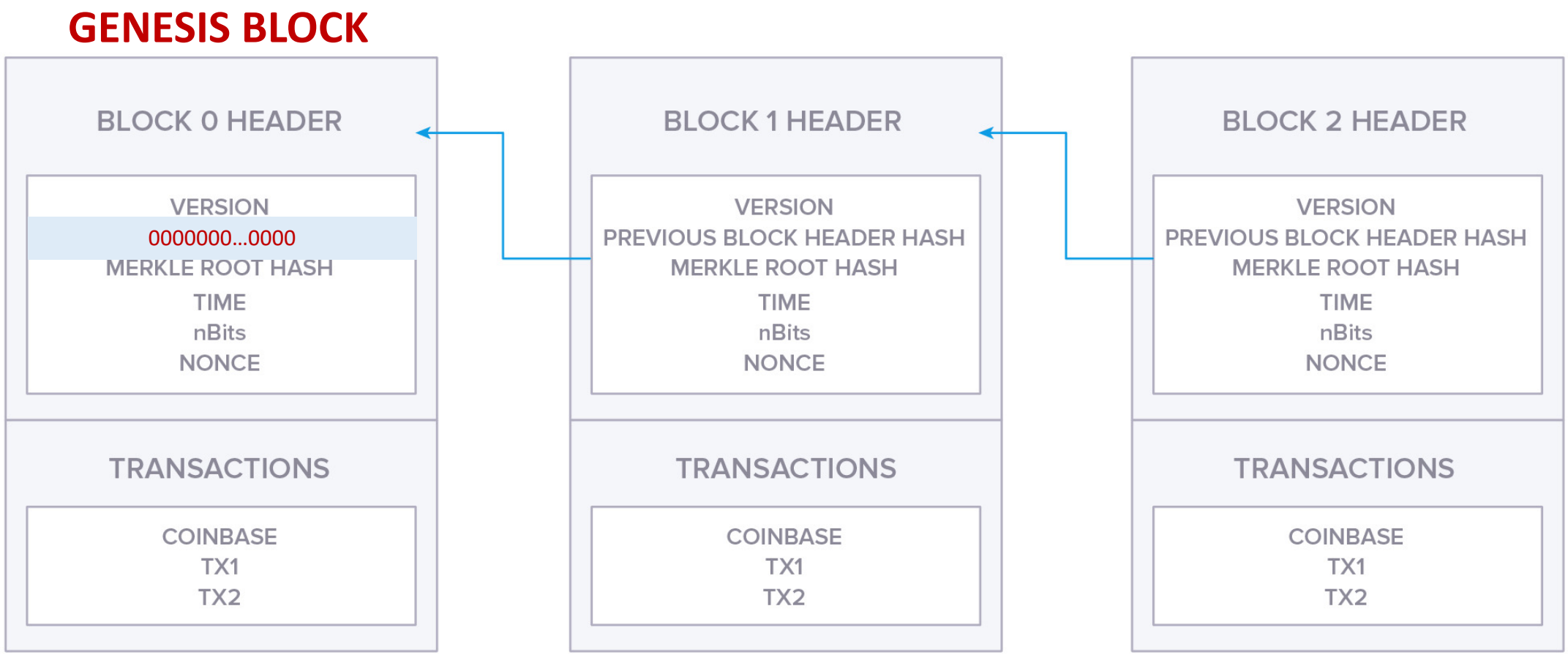
TRANSACTIONS

New Transaction
TO FROM VALUE INPUT OUTPUT SIGNATURE

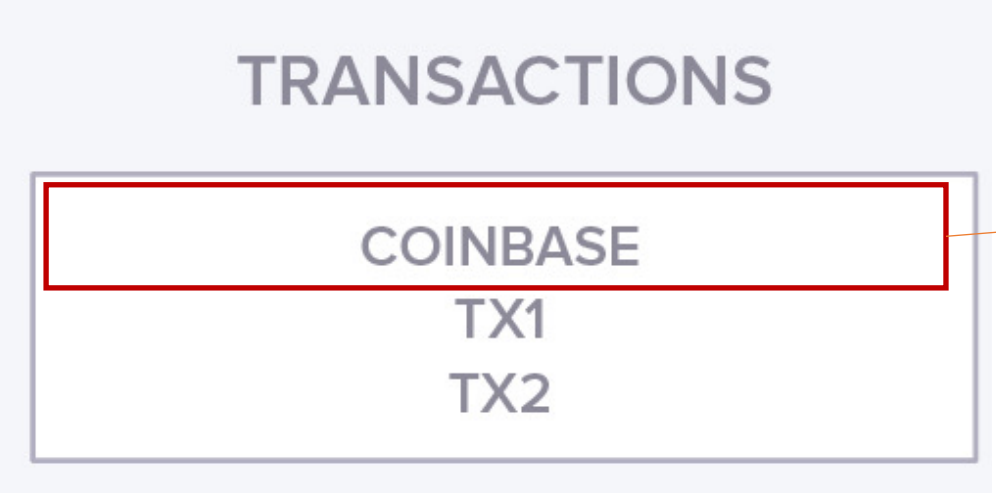
Block number 100	Block number 99	Block number 98
hash previousHash timeStamp nonce	hash previousHash timeStamp nonce	hash previousHash timeStamp nonce
List	List	List
Transaction 1 Transaction 2	Transaction 1 Transaction 2	Transaction 1 Transaction 2 ....

COINBASE TRANSACTION

RECAP



COINBASE TRANSACTION



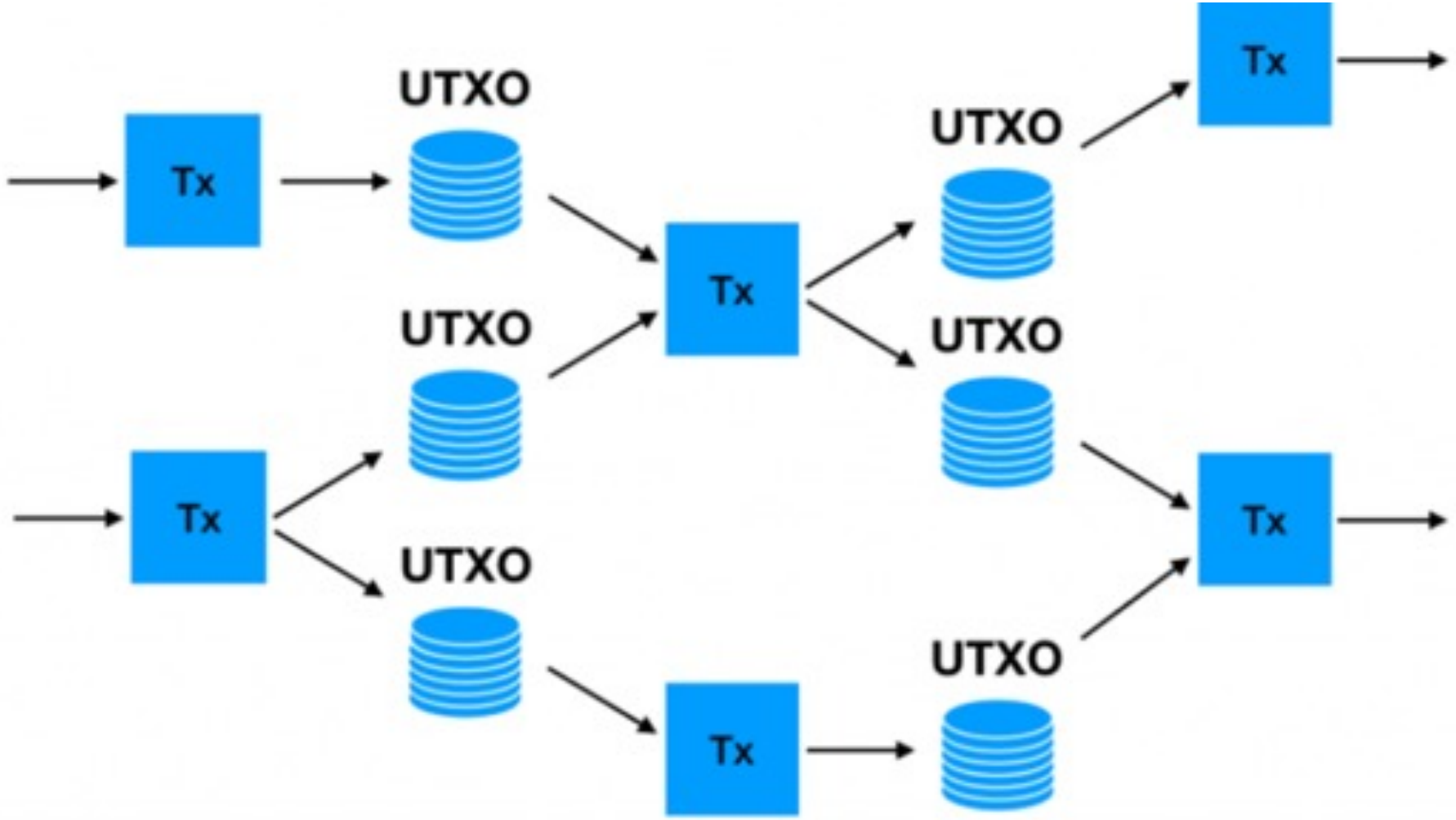
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 405 bytes) (0.000 sat/vByte - 378 virtual bytes)		+6.25107888 BTC
Hash	5254e1e78c5831d99adaac3e67c03180c061...		2022-08-26 13:37
	COINBASE (Newly Generated Coins)	1GNgwA8JfG7Kc8akJ8o...	6.25107888 BTC
		OP_RETURN	0.00000000 BTC
		OP_RETURN	0.00000000 BTC
		OP_RETURN	0.00000000 BTC
		OP_RETURN	0.00000000 BTC

UNSPENT TRANSACTION OUTPUT (UTXO)

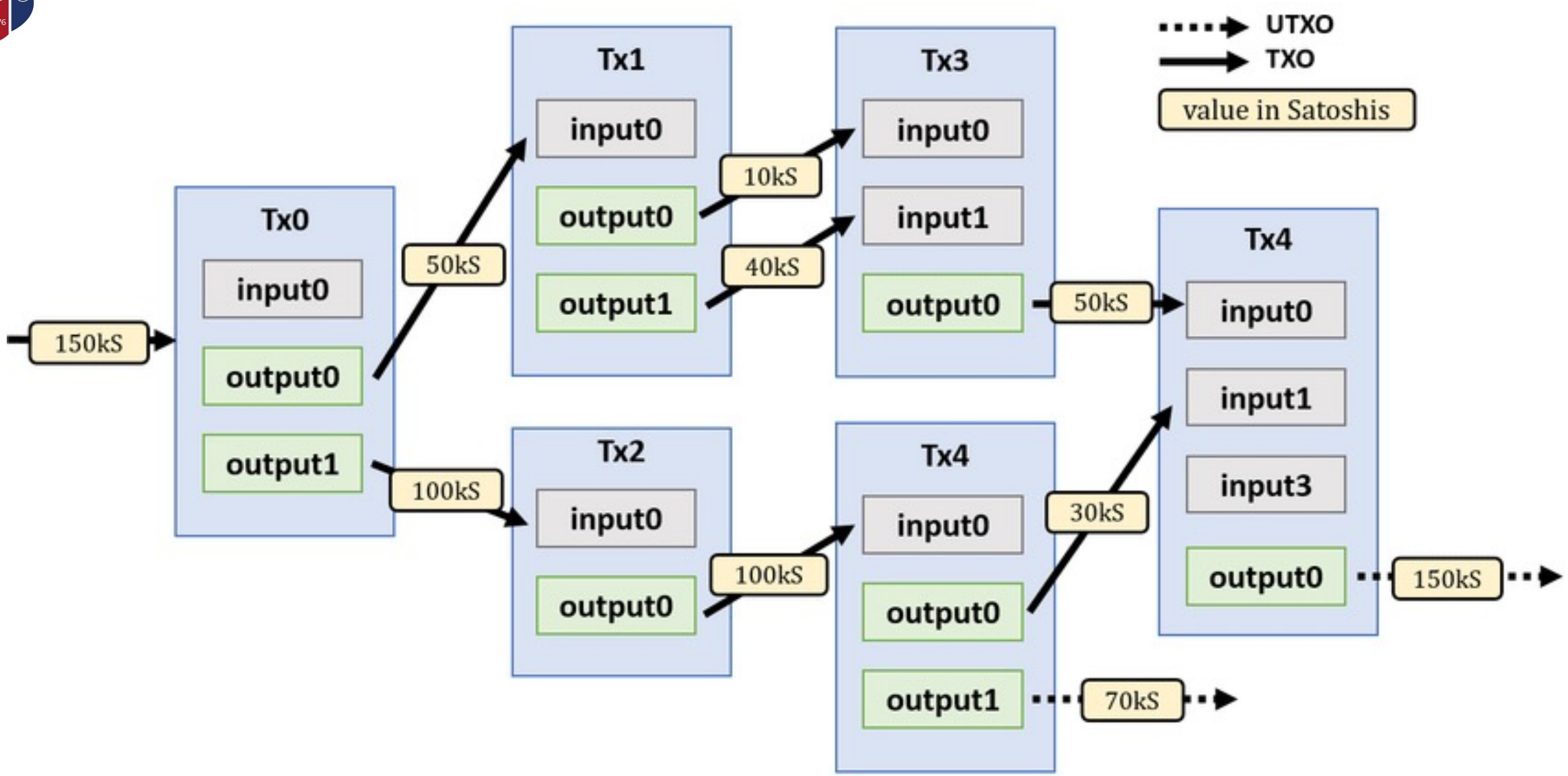
Bitcoin transaction outputs that have not been spent at a given time

- Contains All Currently Unspent Transaction Outputs
- Speeds up Transaction Validation Process
- Stored using a LevelDB database in Bitcoin Core called “chainstate”

UNSPENT TRANSACTION OUTPUT (UTXO)



UNSPENT TRANSACTION OUTPUT (UTXO)



UNSPENT TRANSACTION OUTPUT (UTXO)

BLOCKCHAIN DESIGN