

Quiz: Bitcoin Protocol

Instructions: 21 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?

- A) A user account balance
- B) An unspent transaction output
- C) A unified transaction output
- D) A transaction verification object

Quiz (1-5)

Q1. What is a UTXO in Bitcoin?

- A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object

Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?

- A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000

Quiz (1-5)

Q1. What is a UTXO in Bitcoin?

- A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object

Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?

- A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000

Answer: C – 1 BTC = 100,000,000 satoshis (smallest unit).

Q3. Which component is NOT part of a transaction input?

- A) Previous transaction hash B) Output index C) ScriptPubKey D) ScriptSig

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?

- A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object

Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?

- A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000

Answer: C – 1 BTC = 100,000,000 satoshis (smallest unit).

Q3. Which component is NOT part of a transaction input?

- A) Previous transaction hash B) Output index C) ScriptPubKey D) ScriptSig

Answer: C – ScriptPubKey is in the output, not input. Inputs have ScriptSig (unlocking script).

Q4. How is the transaction fee calculated?

- A) Fixed 0.001 BTC B) Sum of inputs minus sum of outputs C) Explicitly stated in tx D) Based on block height

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?

- A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object

Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?

- A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000

Answer: C – 1 BTC = 100,000,000 satoshis (smallest unit).

Q3. Which component is NOT part of a transaction input?

- A) Previous transaction hash B) Output index C) ScriptPubKey D) ScriptSig

Answer: C – ScriptPubKey is in the output, not input. Inputs have ScriptSig (unlocking script).

Q4. How is the transaction fee calculated?

- A) Fixed 0.001 BTC B) Sum of inputs minus sum of outputs C) Explicitly stated in tx D) Based on block height

Answer: B – Fee is implicit: total input value minus total output value.

Q5. What happens to a UTXO when it is spent?

- A) Balance decremented B) Marked as spent C) Consumed entirely D) Split into smaller pieces

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?

- A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object

Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?

- A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000

Answer: C – 1 BTC = 100,000,000 satoshis (smallest unit).

Q3. Which component is NOT part of a transaction input?

- A) Previous transaction hash B) Output index C) ScriptPubKey D) ScriptSig

Answer: C – ScriptPubKey is in the output, not input. Inputs have ScriptSig (unlocking script).

Q4. How is the transaction fee calculated?

- A) Fixed 0.001 BTC B) Sum of inputs minus sum of outputs C) Explicitly stated in tx D) Based on block height

Answer: B – Fee is implicit: total input value minus total output value.

Q5. What happens to a UTXO when it is spent?

- A) Balance decremented B) Marked as spent C) Consumed entirely D) Split into smaller pieces

Answer: C – UTXOs must be consumed entirely; change is returned via new output.

Q6. What is the purpose of Bitcoin Script?

- A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol

Q6. What is the purpose of Bitcoin Script?

- A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol

Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?

- A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash

Q6. What is the purpose of Bitcoin Script?

- A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol

Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?

- A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash

Answer: B – OP_CHECKSIG verifies the signature using the provided public key.

Q8. Which address format indicates a native SegWit transaction?

- A) Starts with “1” B) Starts with “3” C) Starts with “bc1q” D) Starts with “bc1p”

Q6. What is the purpose of Bitcoin Script?

- A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol

Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?

- A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash

Answer: B – OP_CHECKSIG verifies the signature using the provided public key.

Q8. Which address format indicates a native SegWit transaction?

- A) Starts with “1” B) Starts with “3” C) Starts with “bc1q” D) Starts with “bc1p”

Answer: C – “bc1q” addresses use Bech32 encoding for native SegWit (P2WPKH).

Q9. What problem does SegWit solve?

- A) High fees B) Transaction malleability C) 51% attacks D) Double spending

Q6. What is the purpose of Bitcoin Script?

- A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol

Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?

- A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash

Answer: B – OP_CHECKSIG verifies the signature using the provided public key.

Q8. Which address format indicates a native SegWit transaction?

- A) Starts with “1” B) Starts with “3” C) Starts with “bc1q” D) Starts with “bc1p”

Answer: C – “bc1q” addresses use Bech32 encoding for native SegWit (P2WPKH).

Q9. What problem does SegWit solve?

- A) High fees B) Transaction malleability C) 51% attacks D) Double spending

Answer: B – SegWit fixes transaction malleability by separating witness data from transaction ID.

Q10. How many confirmations are typically considered final for a Bitcoin transaction?

- A) 1 B) 3 C) 6 D) 12

Q6. What is the purpose of Bitcoin Script?

- A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol

Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?

- A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash

Answer: B – OP_CHECKSIG verifies the signature using the provided public key.

Q8. Which address format indicates a native SegWit transaction?

- A) Starts with “1” B) Starts with “3” C) Starts with “bc1q” D) Starts with “bc1p”

Answer: C – “bc1q” addresses use Bech32 encoding for native SegWit (P2WPKH).

Q9. What problem does SegWit solve?

- A) High fees B) Transaction malleability C) 51% attacks D) Double spending

Answer: B – SegWit fixes transaction malleability by separating witness data from transaction ID.

Q10. How many confirmations are typically considered final for a Bitcoin transaction?

- A) 1 B) 3 C) 6 D) 12

Answer: C – Six confirmations (about 1 hour) are standard for finality.

Q11. What is the maximum block weight in SegWit?

- A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?

- A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB

Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?

- A) SegWit B) Taproot C) P2SH D) Lightning Network

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?

- A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB

Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?

- A) SegWit B) Taproot C) P2SH D) Lightning Network

Answer: B – Taproot (2021) introduced Schnorr signatures for efficiency and privacy.

Q13. What is the maturity rule for coinbase transactions?

- A) 10 confirmations B) 50 confirmations C) 100 confirmations D) 144 confirmations

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?

- A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB

Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?

- A) SegWit B) Taproot C) P2SH D) Lightning Network

Answer: B – Taproot (2021) introduced Schnorr signatures for efficiency and privacy.

Q13. What is the maturity rule for coinbase transactions?

- A) 10 confirmations B) 50 confirmations C) 100 confirmations D) 144 confirmations

Answer: C – Coinbase outputs must wait 100 confirmations before being spent.

Q14. What does RBF (Replace-by-Fee) allow?

- A) Cancel any transaction B) Replace unconfirmed tx with higher fee C) Refund fees D) Merge transactions

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?

- A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB

Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?

- A) SegWit B) Taproot C) P2SH D) Lightning Network

Answer: B – Taproot (2021) introduced Schnorr signatures for efficiency and privacy.

Q13. What is the maturity rule for coinbase transactions?

- A) 10 confirmations B) 50 confirmations C) 100 confirmations D) 144 confirmations

Answer: C – Coinbase outputs must wait 100 confirmations before being spent.

Q14. What does RBF (Replace-by-Fee) allow?

- A) Cancel any transaction B) Replace unconfirmed tx with higher fee C) Refund fees D) Merge transactions

Answer: B – RBF (BIP 125) allows replacing unconfirmed transactions with higher-fee versions.

Q15. How often does Bitcoin halving occur?

- A) Every year B) Every 100,000 blocks C) Every 210,000 blocks D) Every 500,000 blocks

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?

- A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB

Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?

- A) SegWit B) Taproot C) P2SH D) Lightning Network

Answer: B – Taproot (2021) introduced Schnorr signatures for efficiency and privacy.

Q13. What is the maturity rule for coinbase transactions?

- A) 10 confirmations B) 50 confirmations C) 100 confirmations D) 144 confirmations

Answer: C – Coinbase outputs must wait 100 confirmations before being spent.

Q14. What does RBF (Replace-by-Fee) allow?

- A) Cancel any transaction B) Replace unconfirmed tx with higher fee C) Refund fees D) Merge transactions

Answer: B – RBF (BIP 125) allows replacing unconfirmed transactions with higher-fee versions.

Q15. How often does Bitcoin halving occur?

- A) Every year B) Every 100,000 blocks C) Every 210,000 blocks D) Every 500,000 blocks

Answer: C – Halving occurs every 210,000 blocks (approximately every 4 years).

Q16. What is the first transaction in every Bitcoin block called?

- A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction

Q16. What is the first transaction in every Bitcoin block called?

- A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction

Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CFP (Child-Pays-for-Parent)?

- A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection

Q16. What is the first transaction in every Bitcoin block called?

- A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction

Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?

- A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection

Answer: B – CPFP allows recipient to create high-fee tx spending unconfirmed output.

Q18. Which Bitcoin upgrade was activated in 2021?

- A) SegWit B) Lightning C) Taproot D) P2SH

Q16. What is the first transaction in every Bitcoin block called?

- A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction

Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?

- A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection

Answer: B – CPFP allows recipient to create high-fee tx spending unconfirmed output.

Q18. Which Bitcoin upgrade was activated in 2021?

- A) SegWit B) Lightning C) Taproot D) P2SH

Answer: C – Taproot (SegWit v1) was activated in November 2021.

Q19. What does P2SH stand for?

- A) Pay-to-Script-Hash B) Pay-to-Secure-Hash C) Peer-to-Script-Hash D) Protocol-to-Script-Hash

Q16. What is the first transaction in every Bitcoin block called?

- A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction

Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?

- A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection

Answer: B – CPFP allows recipient to create high-fee tx spending unconfirmed output.

Q18. Which Bitcoin upgrade was activated in 2021?

- A) SegWit B) Lightning C) Taproot D) P2SH

Answer: C – Taproot (SegWit v1) was activated in November 2021.

Q19. What does P2SH stand for?

- A) Pay-to-Script-Hash B) Pay-to-Secure-Hash C) Peer-to-Script-Hash D) Protocol-to-Script-Hash

Answer: A – P2SH (Pay-to-Script-Hash) enables complex spending conditions.

Q20. When were spot Bitcoin ETFs approved in the US?

- A) 2020 B) 2022 C) January 2024 D) December 2024

Q16. What is the first transaction in every Bitcoin block called?

- A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction

Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?

- A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection

Answer: B – CPFP allows recipient to create high-fee tx spending unconfirmed output.

Q18. Which Bitcoin upgrade was activated in 2021?

- A) SegWit B) Lightning C) Taproot D) P2SH

Answer: C – Taproot (SegWit v1) was activated in November 2021.

Q19. What does P2SH stand for?

- A) Pay-to-Script-Hash B) Pay-to-Secure-Hash C) Peer-to-Script-Hash D) Protocol-to-Script-Hash

Answer: A – P2SH (Pay-to-Script-Hash) enables complex spending conditions.

Q20. When were spot Bitcoin ETFs approved in the US?

- A) 2020 B) 2022 C) January 2024 D) December 2024

Answer: C – SEC approved 11 spot Bitcoin ETFs on January 10, 2024.

Q21. How many confirmations are typically considered final?

- A) 1 B) 3 C) 6 D) 12

Q21. How many confirmations are typically considered final?

- A) 1 B) 3 C) 6 D) 12

Answer: C – Six confirmations (about 1 hour) are standard for finality.