perplexity

6 blocks completion rule

The **6 blocks completion rule** in Bitcoin refers to the widely accepted practice of considering a transaction as *final* or *highly secure* after it has received six confirmations—that is, after six additional blocks have been added on top of the block containing the transaction[1] [2] [3] [4].

What Does "6 Confirmations" Mean?

- **1 confirmation**: Your transaction is included in a block.
- **2 confirmations**: Another block is mined on top of the block containing your transaction.
- ...
- **6 confirmations**: Five more blocks have been mined on top of the block containing your transaction, making it six blocks deep in the blockchain[1] [3] [4].

Why 6 Blocks?

- The choice of 6 is a **security convention**. Each new block added on top of your transaction's block makes it exponentially harder for an attacker to reverse that transaction through a chain reorganization (i.e., a double-spend attack)[1] [5] [4].
- The probability of a successful double-spend drops dramatically with each additional confirmation. With 6 confirmations, the risk is considered negligible for most practical purposes, assuming an attacker controls less than 10% of the network's mining power[5].
- For extremely high-value transactions or if an attacker controls more hash power, more confirmations may be required for similar security[5].

How Long Does It Take?

- Since a new block is mined roughly every 10 minutes, **6 confirmations usually take about 1 hour** on average[4].
- However, because mining is probabilistic, the actual time can be shorter or longer.

Is 6 Blocks a Hard Rule?

- **No, it's a convention**, not a protocol requirement. Merchants and exchanges can set their own thresholds based on the value of the transaction and their risk tolerance[1] [3].
- For small transactions, fewer confirmations may be acceptable. For very large transactions, more may be required.

Example

- Alice sends 1 BTC to Bob.
- The transaction is included in block #800,000. This is the **first confirmation**.
- When block #800,001 is mined, that's the **second confirmation**.
- When block #800,005 is mined, the transaction has **six confirmations** and is considered highly secure.

Technical Note

- **Freshly-mined coins** (the block reward) cannot be spent until they have 100 confirmations, adding an extra layer of security for coin issuance[1].

In summary:
The "6 blocks completion rule" means a transaction is considered final after six blocks have been added on top of the block containing it, making reversal extremely unlikely and providing strong security against double-spending[1] [5] [2] [3] [4].

⁂

1. https://en.bitcoin.it/wiki/Confirmation
2. https://www.tec.gov.in/pdf/Studypaper/Security aspects of blockchain.pdf
3. https://www.reddit.com/r/BitcoinBeginners/comments/r75u8d/what_is_a_confirmation_in_bitcoin/
4. https://www.coincenter.org/education/crypto-regulation-faq/how-long-does-it-take-for-a-bitcoin-transaction-to-be-confirmed/
5. https://bitcoin.stackexchange.com/questions/1170/why-is-6-the-number-of-confirms-that-is-considered-secure