perplexity

What are the risks if I accept a transaction before it reaches 6 confirmations

If you accept a Bitcoin transaction **before it reaches 6 confirmations**, you are exposing yourself to certain risks, primarily the possibility of a **double-spend attack** or a blockchain reorganization that could reverse the transaction.

Key Risks

1. Double-Spending

- Before a transaction has multiple confirmations, there is a risk that the sender could attempt to spend the same bitcoins in two different transactions (a double-spend).
- If a malicious actor controls enough mining power, they could try to create an alternative blockchain branch that excludes your transaction, making it as if it never happened[1] [2] [3].

2. Blockchain Reorganization (Reorg)

- Occasionally, two miners may find a new block at the same time, causing a temporary fork in the blockchain.
- If the block containing your transaction is not on the longest chain after the fork is resolved, your transaction could be dropped and returned to the mempool, making it unconfirmed again[2] [4].

3. Probability of Reversal

- With each additional confirmation, the likelihood of a successful attack or accidental reversal drops exponentially.
- Satoshi Nakamoto's original paper calculated that after 6 confirmations, the probability of an attacker with less than 10% of the network's mining power successfully reversing a transaction is less than 0.1% (1 in 1,000)[1] [2].
- Fewer confirmations mean higher risk; for very small transactions, merchants may accept 0–1 confirmation, but for larger amounts, 6 or more is the standard[2] [4] [5].

Practical Implications

- **Small transactions:** For low-value purchases (e.g., coffee), merchants may accept 0–1 confirmation, accepting some risk for convenience[2] [5].
- **Large transactions:** For high-value transfers, waiting for 6 confirmations is strongly recommended, as the risk of reversal becomes negligible[2] [4].

- **Exchanges and services:** Most major exchanges and payment processors require 3–6 confirmations before crediting deposits to user accounts[2] [6] [7].

Example

- Alice sends Bob 1 BTC.
- Bob sees the transaction in the mempool (0 confirmations). He delivers goods to Alice immediately.
- If a malicious actor or a network fork causes that transaction to be excluded from the main chain, Bob could lose his goods and never receive the BTC.
- If Bob waits for 6 confirmations, the risk of this happening is extremely low—almost impossible under normal network conditions[1] [2] [4].

Conclusion

Accepting a transaction before 6 confirmations increases your risk of loss due to double-spending or blockchain reorganization. The more confirmations, the more secure and irreversible the transaction becomes. Six confirmations is the industry standard for high-value transactions because it reduces the risk to a negligible level[1] [2] [4].

> "A transaction should not be considered as confirmed until it is a certain number of blocks deep... Most exchanges and other merchants who bear the risk from double spending require 6 or more blocks."[2]

> "Satoshi's paper outlines the number of confirmations necessary to be 99.9% sure (less than 1 in 1000 chance of success) that an attacker couldn't build a longer chain to reverse the transaction."[1]

⁂

1. https://bitcoin.stackexchange.com/questions/1170/why-is-6-the-number-of-confirms-that-is-considered-secure
2. https://en.bitcoin.it/wiki/Confirmation
3. https://coinmarketcap.com/academy/article/how-long-does-a-bitcoin-transaction-take
4. https://www.osl.com/hk-en/academy/article/bitcoin-transaction-confirmations-what-to-know-about-receiving-btc
5. https://www.reddit.com/r/Bitcoin/comments/1ba6uc/why_do_we_wait_for_6_confirmations_what_is_it/
6. https://support.kraken.com/articles/203325283-cryptocurrency-deposit-processing-times
7. https://bitflyer.com/en-eu/faq/23-25