perplexity

Confirmed vs. Unconfirmed Transactions

- **Unconfirmed Transactions:**
  These are transactions that have been broadcast to the blockchain network but have not yet been included in a block. When you send a transaction (e.g., sending Bitcoin), it is first checked for validity and then placed in a waiting area called the **mempool**. Until a miner picks it up and includes it in a block, it remains unconfirmed[1] [2] [3].
- **Confirmed Transactions:**
  Once a transaction is included in a block that has been successfully mined and added to the blockchain, it becomes confirmed. Each subsequent block added after this increases the number of confirmations, making the transaction more secure and irreversible[1] [2].

What Is the Mempool?

- The **mempool** (short for "memory pool") is a temporary storage area on each blockchain node where unconfirmed transactions wait to be validated and included in a block. Think of it as a waiting room for transactions[4] [3].
- Each node maintains its own version of the mempool, so the contents may vary slightly between nodes due to network delays or differences in transaction propagation[4] [3].

How Do Miners Select Transactions?

- **Selection Process:**
  Miners are free to choose which transactions from the mempool they want to include in the next block. However, most miners are economically motivated to maximize their rewards, so they prioritize transactions offering the highest fees[5] [6] [7].
- **Block Size Limitation:**
  If the mempool has more transactions than can fit in a block, miners select the highest-fee transactions first, filling the block up to its maximum size[5].
- **Ancestor Rule:**
  If a transaction depends on another (parent/child relationship), miners must include the parent transaction first, which can affect their selection strategy[5].

What Does a Miner Do? Step-by-Step

1. **Collect Transactions:**
   The miner gathers unconfirmed transactions from the mempool, usually prioritizing those with the highest fees[5] [7].
2. **Build a Candidate Block:**
   The miner creates a "candidate block" containing the selected transactions, the hash of the previous block, a timestamp, and a special field called the **nonce**[8] [9].

3. **Start Mining (Proof of Work):**
   The miner repeatedly changes the nonce and hashes the block header (using SHA-256 in Bitcoin) to try to produce a hash that meets the network's difficulty target (e.g., a hash with a certain number of leading zeros)[10] [11] [8].
4. **Broadcast the Block:**
   Once a miner finds a valid nonce, the new block is broadcast to the network. Other nodes verify the block and, if it's valid, add it to their copy of the blockchain. The transactions in this block are now confirmed[10] [8].
5. **Receive Rewards:**
   The miner receives the block reward and transaction fees from the transactions included in the block[7].

Can Miners Precompute Nonces for Leading Zeros?

- **No, Precomputation Is Not Possible:**
  The process is inherently random and unpredictable due to the cryptographic properties of the hash function (SHA-256). There is no shortcut—miners must use brute force, trying different nonce values until a valid hash is found[10] [11] [8].
- **No Prefix or Special Pattern Added:**
  The requirement is that the resulting hash of the block header (which includes the nonce) must be below a certain target value (often visualized as having a set number of leading zeros). There's no way to predict which nonce will work; the only approach is to try as many as possible[11] [8].

Example

Suppose a miner assembles a block with pending transactions and starts with nonce = 0. The miner hashes the block header:

- If the hash does not have the required number of leading zeros, the miner increments the nonce to 1 and tries again.
- This process repeats—sometimes billions of times—until a valid nonce is found.
- When successful, the block is broadcast, and all included transactions are confirmed[10] [11] [8].

Summary Table

Concept	Description
Unconfirmed Transaction	Awaiting inclusion in a block, stored in the mempool[1] [2] [3]
Confirmed Transaction	Included in a block on the blockchain[1] [2]
Mempool	Temporary storage for unconfirmed transactions on each node[4] [3]
Miner Transaction Choice	Picks highest-fee transactions, must include parents first[5] [6] [7]
Mining Process	Repeatedly hashes block header with different nonces to find a valid hash[10] [11] [8]

Concept	Description
Precomputing Nonce	Not possible; brute-force search is required [10] [11] [8]
Miner’s Reward	Block reward + transaction fees [7]

This process ensures the security, fairness, and integrity of blockchain networks.

⁂

1. https://www.cyfrin.io/blog/what-is-a-blockchain-unconfirmed-transaction
2. https://www.ledger.com/academy/glossary/unconfirmed-transaction
3. https://cryptonews.com/academy/mempool/
4. https://www.risein.com/blog/blockchains-waiting-room-mempool
5. https://learnmeabitcoin.com/technical/mining/candidate-block/
6. https://ethereum.stackexchange.com/questions/76705/how-do-miner-choose-transactions-for-a-block
7. https://bitcoin.stackexchange.com/questions/57823/how-do-miners-choose-transactions
8. https://blog.whitebit.com/en/ethereum-nonce-explained/
9. https://wesecureapp.com/blog/nonce-the-core-of-blockchain-security/
10. https://cointelegraph.com/explained/what-is-a-nonce-in-blockchain-explained
11. https://coincentral.com/what-is-a-nonce-proof-of-work/