perplexity

Double Spend: Banks vs Blockchain

In Banks (UPI, Cards)

- **Double spending** in traditional banking (including UPI and cards) means trying to spend the same money more than once before the system updates the balance.
- **Prevention in Banks:**
  - Centralized ledgers: Banks and payment processors maintain a single source of truth about account balances.
  - Real-time transaction checks: When you pay via UPI or card, the system instantly verifies if you have enough funds, deducts the amount, and prevents simultaneous double use.
  - Settlement systems: Even if there's a brief lag, backend reconciliation ensures only one transaction is finalized if there's a conflict[1] [2].

Example:
If you try to pay ₹1,000 to two people at the same time using UPI, only one will succeed; the other will fail due to insufficient balance.

In Blockchain

- **Double spending** in blockchain means trying to spend the same cryptocurrency twice by broadcasting two conflicting transactions.
- **Prevention in Blockchain:**
  - **Decentralized ledger:** Every node keeps a copy of all transactions.
  - **Consensus mechanism:** Transactions are grouped into blocks; only one valid transaction spending a given coin can be confirmed in the chain.
  - **Proof-of-Work (PoW):** Miners compete to add blocks, ensuring only one version of history is accepted.
  - **Block confirmations:** Once a transaction is included in a block and more blocks are added on top, reversing it (and thus double spending) becomes exponentially harder[3] [4] [5] [6].

Example:
If Alice tries to send the same bitcoin to Bob and Carol, only the transaction included in the next block will be confirmed; the other will be rejected as invalid.

What Is a Merkle Root?

- The **merkle root** is a single hash that summarizes all transactions in a block.
- It is created by repeatedly hashing pairs of transaction IDs (TXIDs) together in a tree structure until only one hash remains—the merkle root[7] [8].
- The merkle root is stored in the block header and ensures that even a tiny change in any transaction will change the root, protecting the block's integrity.

Example:
If a block has 4 transactions (A, B, C, D):

- Hash A and B → AB
- Hash C and D → CD
- Hash AB and CD → Merkle root

Parts of a Blockchain Block

Part	Description
Block Header	Metadata summarizing the block (see below)
Block Body	List of transactions included in the block
Transaction Counter	Number of transactions in the block

What Does a Block Header Contain?

A typical block header (e.g., Bitcoin) includes[9] [10] [11] [12]:

- **Version:** Protocol version used.
- **Previous Block Hash:** Hash of the preceding block (links blocks together).
- **Merkle Root:** Hash summarizing all transactions in the block.
- **Timestamp:** When the block was created.
- **Difficulty Target:** How hard it is to find a valid block.
- **Nonce:** Number miners adjust to find a valid hash.

Is Only the Block Header Used When Mining?

- **Yes.** Miners only hash the block header (not the entire block) when searching for a valid block hash.
- This is efficient because the header is much smaller than the full block, and any change in transactions (affecting the merkle root) or other header fields changes the hash[10] [11].

Does a Block Store Its Own Hash?

- **No, a block does not store its own hash inside itself.**
- Instead, a block's hash is calculated from its header and is used as a reference by the *next* block.
- The hash of each block is stored in the header of the following block (as the "previous block hash"), creating the chain[11] [13].

Example:

- Block #100's hash is stored in Block #101's header as the "previous block hash".
- This chaining ensures tamper-evidence: changing any data in Block #100 changes its hash, breaking the chain.

Example Table: Block Structure

Field	Where Stored	Purpose
Block Hash	Not inside block; calculated and stored in next block's header	Unique fingerprint for the block
Previous Block Hash	Block header	Links to previous block, forms the chain
Merkle Root	Block header	Summarizes all transactions in the block
Timestamp	Block header	Time block was created
Nonce	Block header	Used for mining (proof-of-work)
Transactions	Block body	All included transactions

Summary

- **Banks prevent double spending** via centralized ledgers and instant balance checks.
- **Blockchain prevents double spending** using decentralized consensus, block confirmations, and cryptography.
- **Merkle root** efficiently summarizes all transactions in a block.
- **Block header** contains key metadata (previous hash, merkle root, timestamp, etc.), and only the header is hashed during mining.
- **A block does not store its own hash**; its hash is referenced by the next block, ensuring immutability and security of the blockchain[3] [4] [7] [9] [10] [11] [5] [6] [13].

⁂

1. https://cleartax.in/s/upi-transaction-charges
2. https://www.npci.org.in/what-we-do/upi/faqs
3. https://www.coingecko.com/learn/double-spending

4. https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp
5. https://www.financestrategists.com/wealth-management/blockchain/double-spending-in-blockchain/
6. https://www.bitget.com/wiki/double-spending-in-a-peer-to-peer-system-and-how-blockchain-mitigates-it
7. https://learnmeabitcoin.com/technical/block/merkle-root/
8. https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp
9. https://www.theblock.co/learn/245697/what-are-blocks-in-a-blockchain
10. https://www.ledger.com/academy/glossary/block-header
11. https://www.educative.io/answers/how-do-block-hashes-work-in-blockchain
12. https://www.investopedia.com/terms/b/block-header-cryptocurrency.asp
13. https://learnmeabitcoin.com/technical/block/hash/