End-to-End Blockchain Transaction Pipeline

USER / WALLET

- **Generate Keypair**
  Private/Public
- **Compose & Sign Tx**
  (to, amount, fee, nonce/data)
- **Broadcast Raw Tx**
  → P2P peers

FULL NODES (PEERS) — Transaction Verification

- **Verify Tx**
  • Signature valid
  • Balance/UTXO or nonce ok
  • Format/policy/fee ok

"Valid?" — Yes → **Add to Mempool** / No → **Reject Tx**

BLOCK PRODUCER (Miner / Validator)

- **Select Mempool Tx**
  (fee, size, rules)
- **Build Candidate Block**
  Header + Merkle Root + Tx List

CONSENSUS & BLOCK VALIDATION

- **Block Validation**
  Recheck txs, header, parent, structure

- **PoW**
  Find nonce: H(header) < target
- **PoS**
  Proposer/Committee, attestations, finality

⚠ **51% Attack Surface**
- PoW: >51% hashpower → censor/reorg/double-spend their own tx
- PoS: >51% stake/committee → malicious finalization/censorship
- *Cannot forge signatures or create funds*

PROPAGATION & FORK CHOICE

- **Gossip Proposed Block** → Peers
- **Peers Validate & Fork-Choice**
  Longest/Heaviest/Finality rule

"Canonical?" — Yes → **Append Block to Local Chain** / No → **Hold Competing Fork / Wait**

CONFIRMATIONS / FINALITY

- **Accrue Confirmations** (BTC) or
  Finality (PoS checkpoints)

"Final/Deep?" — Yes → **State Update**
Balances/UTXOs/Storage/Logs / No → **Reorg Risk Persists**

LAYER-2 (Optional)

"Use L2?" — Lightning

- **Lightning**
  Open channel (L1 funding)
- Off-chain HTLC updates (fast/low fee)
- Close channel → Settle on L1

Security inherits L1; penalty/justice tx deters cheating.

Optimistic Rollup — No → Proceed purely on L1

- **Optimistic Rollup**
  Send tx to L2 sequencer (fast, low fee)
- Batch posted to L1 (data availability)
- Fraud window → possible fault proofs
- Finalize on L1 → Settle L2 state