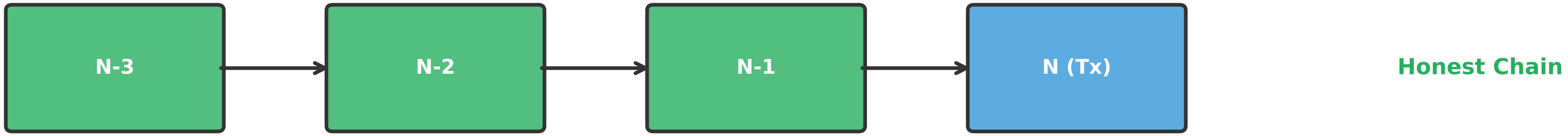
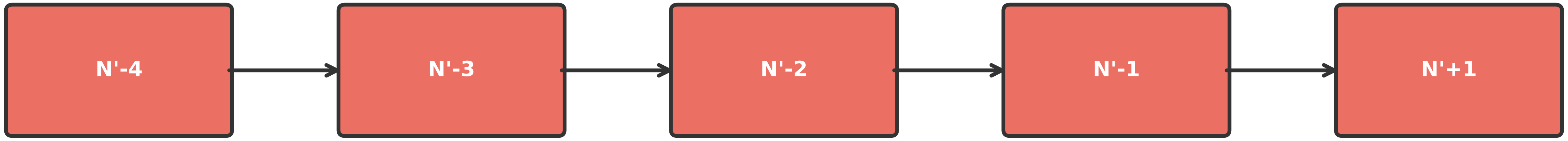
51% Attack: Double Spending via Chain Reorg

Step 1: Attacker sends BTC to exchange (Block N)



Step 2: Attacker secretly mines alternative chain (without Tx)



Secret Attacker Chain (longer = wins)

Cost to attack Bitcoin (2024): ~$1-2 million/hour in electricity + hardware

Step 3: Attacker broadcasts longer chain - network accepts it

RESULT: Original transaction reversed!

Attacker keeps both: BTC + goods/services from exchange

Defense: Wait for 6+ confirmations before accepting large payments

Source: Crypto51.app, Bitcoin Security Analysis (2024)