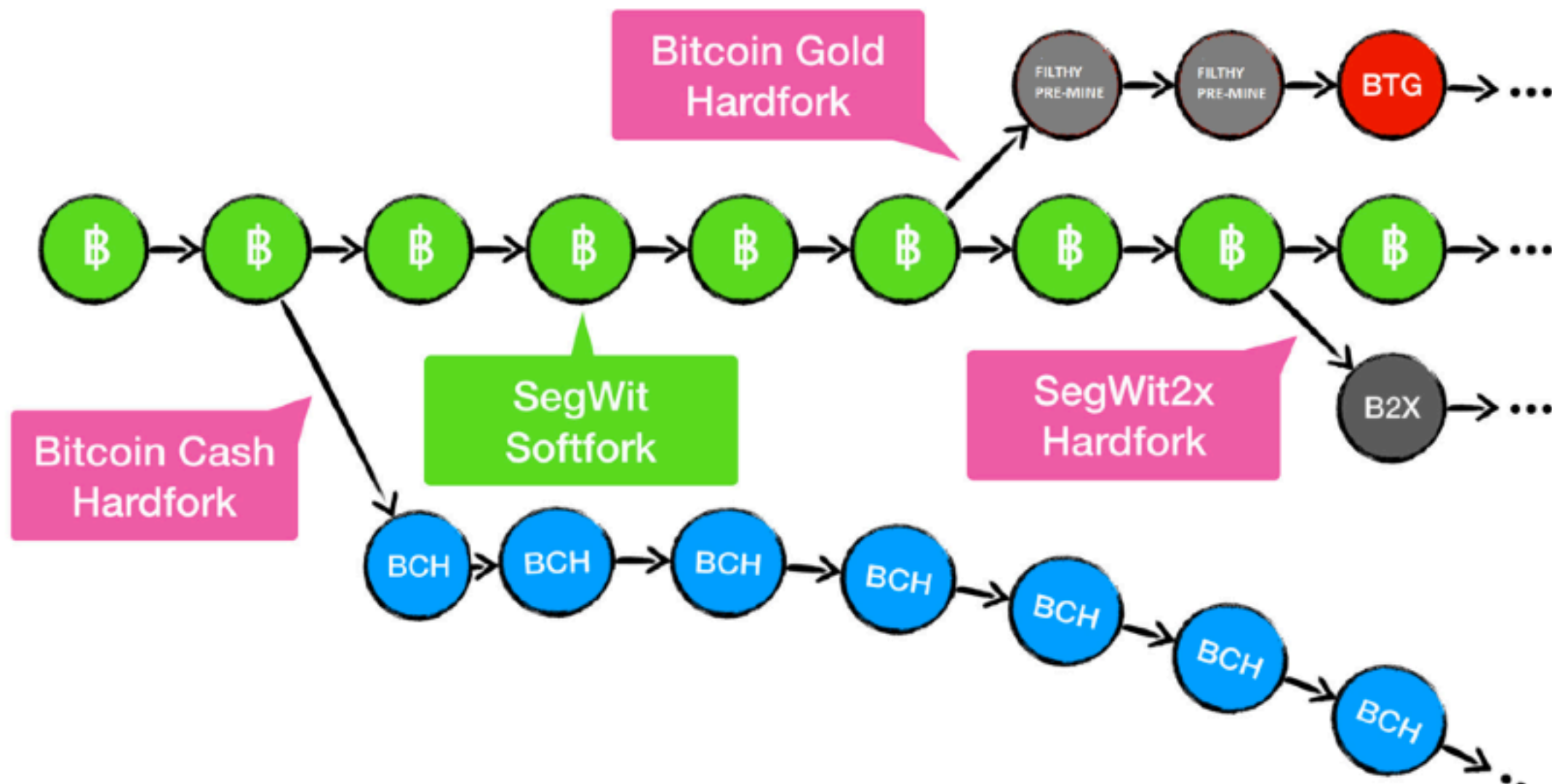


# Bitcoin Forks 2017



# SegWit

## Segregated Witness

- Soft Fork - Bitcoin Improvement Proposal - BIP-91 (supersedes BIP141)
- Solve malleability (can't decipher but can modify the cypher text to produce undesired plaintext decode)
- Works by splitting the transaction into two segments
  - Removes the unlocking signature ("witness" data) from the original tx segment and adds it as a separate structure at the end.
- Original section would continue to hold the sender and receiver data,
  - new "witness" structure would contain scripts and signatures.
  - original data segment would be counted normally,
  - "witness" segment ends up counted as a quarter of its real size.