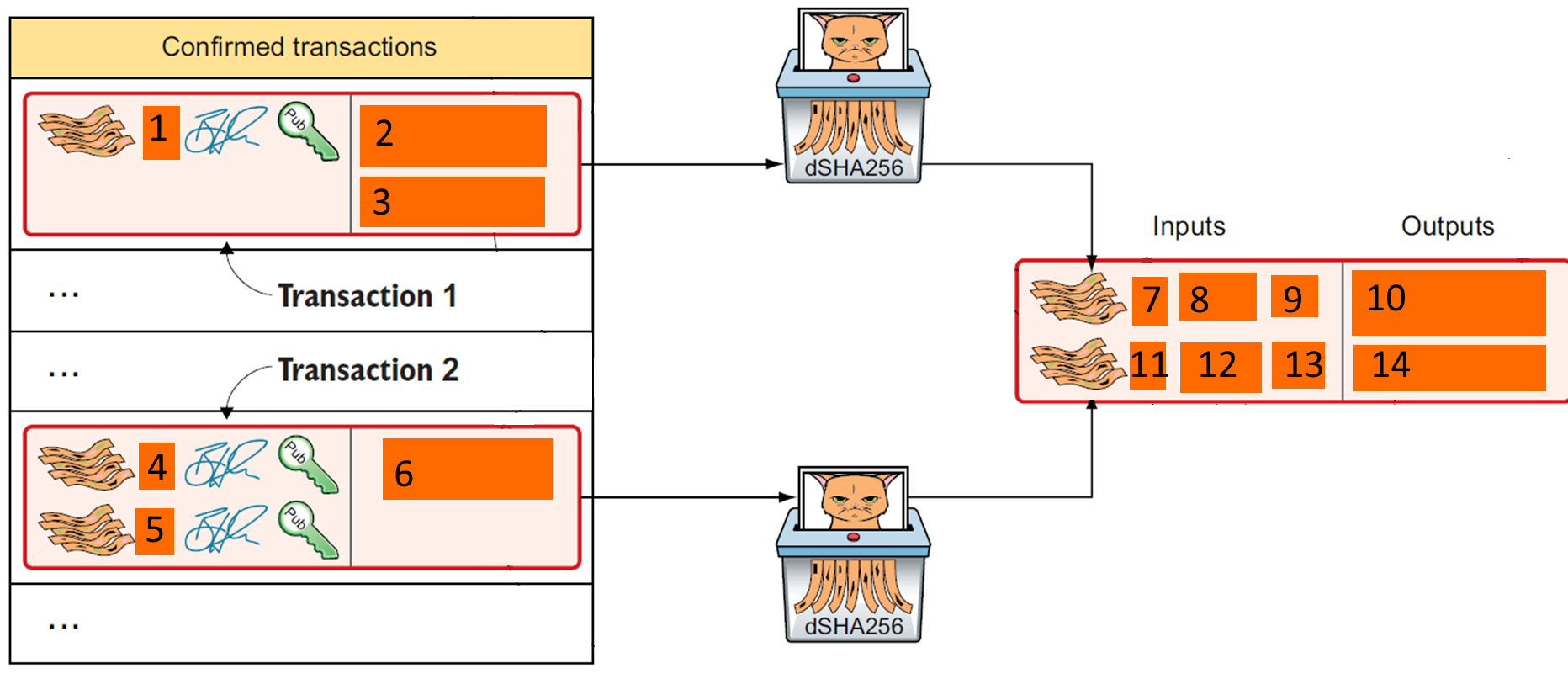
Exercise: Understanding Simplified View of Transactions



The above is a diagram of how a transaction is created from UXTO set. Suppose PKH1, PKH2 and PKH3 belongs to John. And John is going make a transaction to PKHX amounting to 25 coins. John has two UXTO that amounts to 15 and 18 coins [FIXED].

Fill in the above diagram that is labelled 1-14 with the correct information.

|  |  |
| --- | --- |
| No |  |
| 1 | Any number |
| 2 | Any number |
| 3 | 15 PKH1 (2 and 3 can be swapped, then 7 must change accordingly) |
| 4 | Any number |
| 5 | Any number |
| 6 | 18 PKH2 (3 and 6 can be swapped but many other things need to be changed) |
| 7 | 1 (linked to 15 PKH1) |
| 8 | PHK1 digital signature |
| 9 | PHK1 public key |
| 10 | 25 PKHX |
| 11 | 0 (linked to 18 PKH2) |
| 12 | PHK2 digital Signature |
| 13 | PHK2 public key |
| 14 | 8 PHK3 (return change) |