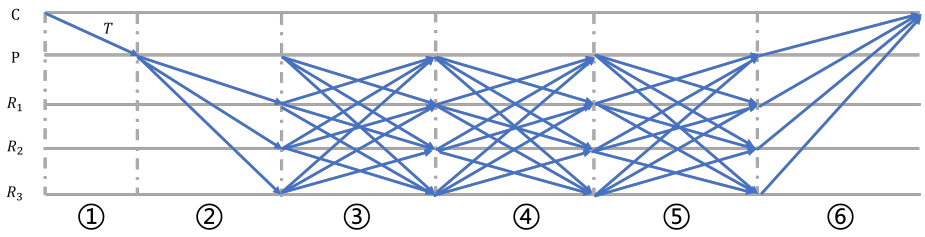

Figure 1: Fit into PBFT protocols.

For R1-O2 and R3-O2:

Theorem 1. *When the percentage of malicious nodes is less than 1/3, the result obtained by BubbleRank satisfies the Condorcet consistency property, which requires that if a transaction has the highest priority in each base order made by non-faulty nodes, it should be ordered with the highest priority in the consensus order.*

Proof. Suppose R is the set of base orders made by non-faulty nodes, R' is the set of base orders made by malicious nodes, and $|x|$ is the number of base orders in x. Thus, $R \geq 2 \cdot |R'|$. Suppose t_g is the transaction with the highest priority in each base order in R. Thus, in the first round of the while-loop, $\alpha_g \leq |R'|$. Besides, for any transaction t_i except t_g, in the first round of the while-loop, $\alpha_i \geq |R| \geq |R'|$. Thus, BubbleRank order t_g with the highest priority, which completes our proof. □

For R2-O3:

For example, our metric and algorithms can fit into PBFT protocols as shown in Figure 1. Compared with traditional PBFT protocols, we add an extra stage, namely base-prepare, between the pre-prepare stage and the prepare stage. Firstly, clients sends transactions to an elected primary (shown by ①). Then, in the pre-prepare stage (shown by ②), the primary sends the collected transaction set to other nodes. After that, in the base-prepare stage (shown by ③), each node generates a set of base orders and sends the base orders to other nodes. Next, in the prepare stage (shown by ④), each node sends the base orders s/he receives to others. If a node receive the same base order from more than 2/3 nodes, she/he thinks it is valid. Then, in the commit stage (shown by ⑤), each node runs the same algorithm (BubbleRank or CrossMerge) over the valid base order set to get a consensus order and sends it to others. Finally, if a node receives the same consensus order from more than 2/3 nodes, s/he can commit this order and reply it to clients (shown by ⑥). If a client receive the same order from more than 1/3 nodes, s/he can confirm that the order is valid.