MANX Public Chain Consensus Protocol

Topic 1: Basic Concepts of MANX Public Chain Consensus

State machine replication, also referred to as "atomic broadcast," is a core abstraction of the distributed system. In a state machine replication protocol, servers seek to agree on a growing, linearly-ordered log.

Two important features must be satisfied:
(1) consistency, i.e., all servers must have the same log records;
(2) liveness, i.e., whenever a node submits a transaction, the transaction can be recorded on the log very quickly.

The term "responsiveness" of a consensus protocol means that the time for an honest node to confirm a transaction depends only on the network delay. Responsiveness is extremely difficult to accomplish.

The MANX team has developed "optimistic responsiveness" that allows MANX to deliver responsiveness under certain key conditions and bounds the timing under all remaining situations. The optimistic-case (under which the protocol provides responsive confirmation) requires that more than 3/4 nodes are honest and online, and the designated player is honest. Alternately, in the worst-case, assuming that at least 2/3 of the nodes are honest, the protocol uses slow confirmation to assure consistency.

Topic 2: Introduction to MANX Consensus Design

The design of MANX consensus is:

- We have a designated node: the leader. Transactions are sent to the leader. The leader signs the transaction (with an increasing sequence number), and sends out the signed transaction to a "committee"
- The committee members confirm the leader-signed transactions with at most one sequence number.
- If a transaction has received more than 3/4 of the committee's signatures—we refer to such a transaction as being notarized
- Participants can directly output their longest sequence of consecutive notarized transactions—all those transactions are confirmed.

This protocol is consistent if 1/2 the committee is honest. In addition, it satisfies liveness

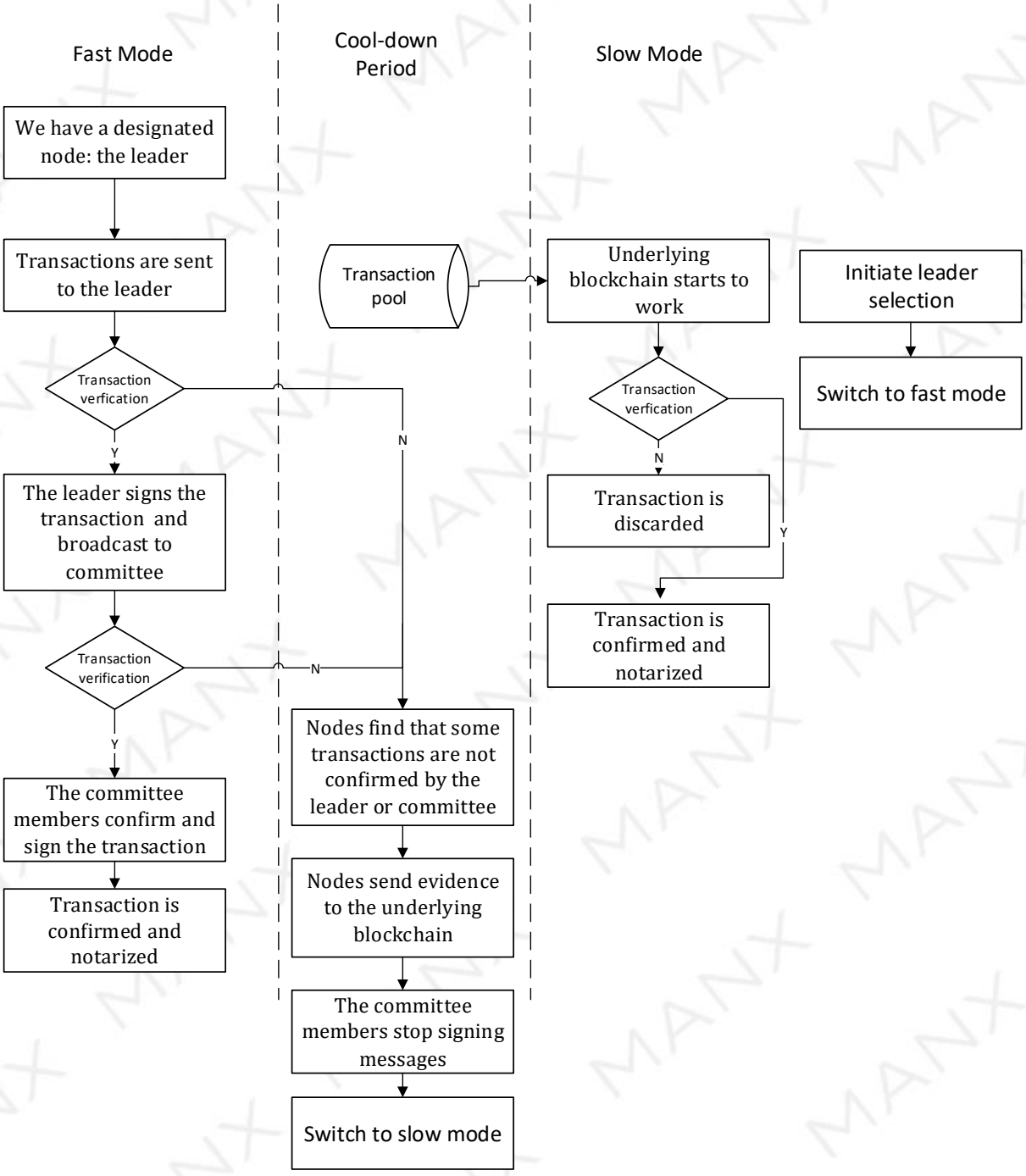
under optimistic-case condition (the leader is honest, and 3/4 of the committee is honest). In fact, under optimistic-case conditions, we only need two communication rounds to confirm a transaction. However, if the leader is cheating, the protocol halts.

If nodes find that some transactions are not confirmed by the leader or committee, evidence is sent to the underlying blockchain. The protocol enters a cool-down period. The committee members stop signing messages sent from the leader, but we allow them to broadcast the notarized transactions.

After the cool-down period ends, the protocol comes to a slow period where transactions can only be confirmed in the underlying blockchain. We can then use the blockchain to replace the leader and start a new optimistic protocol period.

The design of MANX Consensus is extremely simple. Under optimistic conditions, the transaction is confirmed within just one round. Under the worst conditions, the data security and authenticity are ensured in slow mode. Simple design is very important for large-scale distributed systems. MANX can accelerate any existing blockchain, either as an optimistic solution or as a blockchain solution. MANX can withstand 49% attack.

Topic 3: MANX Consensus Flow Chart



MANX Consensus Flow Chart