**Name:** Samiya Kazi

**ID:** 1711620642

**How sharding creates security loopholes**

Instead of the blockchain validating each and every transaction across every node, sharding distributes the workload, and in doing so, opens the door to a single-shard attack. This creates vastly greater opportunities for an attacker, who would now only need to overcome one shard. Once that shard is compromised, the attacker can easily breach other shards. With sharding eliminated from the equation, however, an attacker would have to attack every single machine on the network, which is much harder to do.

Sharding also adds significant poundage to an already complex software stack. It would be like trying to build one skyscraper on top of another. At some point, the structure would likely either tip over or just collapse under its own weight.

Load Balancing Loophole Solutions:

The [MongoDB](https://severalnines.com/product/clustercontrol/for_mongodb) balancer process takes care of distributing your collections evenly across the shards. For example, if one shard of your cluster contains too many chunks of your sharded collection, that particular shard can receive more traffic in comparison to other shards. Therefore, the balancer process balances the chunks of collections properly across the shards. In most of the MongoDB deployments, the default configurations of the balancer process are sufficient enough for normal operations. But, in some situations, database administrators might want to alter the default behavior of this process.

Sources:

<https://severalnines.com/database-blog/guide-configuring-load-balancer-mongodb-sharded-cluster>