Abstract No: SI-13

Introducing a new statistical model to analyse the security of the shard-based public blockchain

N. H. A. C. M. Hangawaththa*

[1]Department of Statistics & Computer Science, Faculty of Science, University of Kelaniya, Sri Lanka
madhuhangawatta@gmail.com*

To support a large amount of data traffic and unyielding quality of service requirements, a highly scalable and reliable networking system is required for public use of blockchain technology. There are several types of studies carried out particularly in developing new methods to use blockchain protocols to manage data transmitted from a larger number of industry segments, such as supply chain, banking, healthcare, and the government sector. Nevertheless, the scalability of the blockchain system remains a problem because of the massive amounts of data generated through the networks. Current blockchain systems are incapable of handling large number of transactions per second (TPS). This results in current blockchain systems being unsuitable for large scale and real-time controlled networks. Recent studies carried out in this area, have proposed the use of shard-based consensus protocols which suggests splitting transactions into multiple committees or shards. These shards are processed in parallel. This parallel processing of split shards or sets of transactions improves the overall scalability, significantly. However, there is not enough scientific literature available to analyse the security of shard-based public blockchain protocols. The key contribution of this study is to introduce a probabilistic model to analyse the security of shard-based public blockchain technology by using the cumulative negative binomial distribution and hypergeometric distribution, based on the failure probability bounds of each committee/epoch. In this study, the classical bound of Chebyshev, Chvátal and Hoeffding bounds are used to evaluate the proposed model with the comparison of three bounds. Furthermore, the popular sharding protocols (Rapid-chain, OmniLedger, Elastico, Harmony and Zilliga) have been analysed to validate the introduced statistical model. The study proposes an approach, via a shard-based blockchain protocol, and defines the conditions that need to be met in order to keep the likelihood of failure smaller than a given threshold.

Keywords: Blockchain, Failure probability bound, Hypergeometric distribution, Negative binomial distribution, Sharding